Cyber, Intelligence, and Security

Volume 3 | No. 1 | May 2019

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
TEL AVIV UNIVERSITY אוניברסיטת תל אביב

Cyber, Intelligence, and Security

Volume 3 | No. 1 | May 2019

Contents

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
TEL AVIV UNIVERSITY אוניברסיטת תל אביב

Cyber, Intelligence, and Security

The purpose of *Cyber, Intelligence, and Security* is to stimulate and enrich the public debate on related issues.

Cyber, Intelligence, and Security is a refereed journal published three times a year within the framework of the Cyber Security Program at the Institute for National Security Studies. Articles are written by INSS researchers and guest contributors. The views presented here are those of the authors alone.

The Institute for National Security Studies is a public benefit company.

Graphic Design: Michal Semo-Kovetz, Yael Bieber, Tel Aviv University Graphic Design Studio
Printing: Elinir

The Institute for National Security Studies (INSS)
40 Haim Levanon • POB 39950 • Tel Aviv 6997556 • Israel
Tel: +972-3-640-0400 • Fax: +972-3-744-7590 • E-mail: info@inss.org.il

Cyber, Intelligence, and Security is published in English and Hebrew.
The full text is available on the Institute's website: www.inss.org.il

ISSN 2519-6677 (print) • E-ISSN 2519-6685 (online)

European Countries Facing the Challenge of Foreign Influence on Democracy—Comparative Research

David Siman-Tov and Mor Buskila

Attempts by countries to influence other countries constitute a security challenge and a threat to democracy. European countries have identified this challenge as a threat to national security and are dealing with it through government actions, civilian activity, and cooperation between countries, reflecting different approaches and proposed solutions to the problem. This article seeks to examine the various methods that the major European countries are using to cope with this challenge and to assess the differences between them by means of their political culture. In addition, this article shows the differences resulting from the strength and type of threat. Thus, it will be possible to speculate about the possibilities and the limits of implementing different coping approaches according to their political-cultural character and whether these approaches can be applied in other countries, including Israel.

Keywords: Europe, Russia, influence, coping strategy, political culture, the battle for minds, democracy

Dudi Siman-Tov researches the field of cognition at INSS. Mor Buskila is a research assistant in the Lipkin-Shahak Program "National Security and Democracy in an Era of Post-Truth and Fake News" at INSS.

Introduction

The international community increasingly has begun to address efforts to exert influence in the digital and network age, particularly following the exposure of Russian attempts to sway the US elections in 2016 as well as their efforts to have influence in many European countries. Attempts to influence are defined as activating the dialogue on values, cultures, and ideas using various tools—including social media and traditional media—in order to change public opinion, disrupt, interfere with processes, and undermine stability.[1] Campaigns of disinformation and manipulation of political and public debate are intended to deepen social rifts, intensify internal and external tensions, undermine public trust in government institutions, and affect strategic decisions or election results in favor of the interests of those behind the campaigns.[2]

This research focuses on different European states in order to understand how they address at the national level efforts to exert influence, which has developed with technological advancements, the rise of social media, and the undermining of the notion of truth. This article does not deal with attempts to influence by individual agents, formal foreign policy, the use of economic tools or demonstrations of military power. Rather, it focuses on efforts to affect cognition by the streaming of information that is false, designed to influence, while using social media as an arena in which new conflicts are conducted. It should be noted that the European states all face different types of threats and challenges. Countries that are geographically closer to Russia have experienced a more significant strategic threat, while Russian-speaking communities have been more exposed to direct influence, and others have experienced a combination of internal and external threats.

Specifically, this research focuses on those countries that are fertile ground for Russian influence, the threats that they face, how they cope with them, and how to explain the differences in methods of coping between the countries. We considered a wide range of objectives and parameters, such as the country's geopolitical conditions, its geopolitical proximity to Russia and

1 Naja Bentzen, "Foreign Influence Operations in the EU," *EPRS – European Parliamentary Research Service*, July 2018, p. 1, https://bit.ly/2ORBBuI.

2 Andrew Weisburd, Clint Watts, and J.M. Berger, "Trolling for Trump: How Russia is Trying to Destroy our Democracy," *War on the Rocks*, November 6, 2016, https://bit.ly/2iyw0fU.

to its strategic routes, the existence of a Russian minority within the country and its connection to Russia, ideological competition, economic interests, and the unique political culture of each. The countries can be divided into three groups: the Baltic states of Estonia, and Latvia; the Nordic states of Sweden and Denmark; and the Western European states of Germany, France, and Britain. This regional division also facilitates the political-cultural research, which indicates shared values of the countries within each group.

Methodological Background

In order to answer the research questions, we have relied on concepts that serve the course of the debate as well as on several research approaches, since the ways in which the threats are perceived in Europe differ from that of the United States or Israel. An important concept used in this research is that of "political culture." Political culture refers to the collection of values, emotions, and perceptions that reflect the nature of a country's political conduct. In comparative research, political culture is an aid to understanding a country's past and present behavior and to forecasting future behavior.[3] This concept facilitates a comparison of how different countries react to the threats, their attitudes to values such as democracy and freedom of expression, and the steps civil society can take to address the threats.

Comparative political research attempts to combine knowledge about different countries and apply it to reality through analysis of political processes and their causes. One possible approach is to look at the political culture.[4] Political culture includes civic orientation at three levels. The first level, the political system, refers to how citizens perceive, accept, and trust the values and organizations constituting the political system. The second level, the process of formulating policy, refers to the expectations of how politics should be conducted and the link between the individual and the political process. The third level, the policies and their inputs and outputs, is also connected to public expectations of government and includes its policy

3 Gabriel Almond, "Political Socialization and Political Culture" in *Comparative Politics Today: A World View,* ed. Gabriel Abraham Almond and G. Bingham Powell (New York: Harper and Collins, 1992), pp. 33–39.

4 M. I. Lichbach and A. S. Zuckerman, "Research Traditions and Theory," in *Comparative Politics: An Introduction*, ed. M. I. Lichbach and A. S. Zuckerman (New York: Cambridge University Press, 2003), pp. 3–9.

goals and how the government works to achieve them.[5] Together, the three levels form the citizens' perceptual framework of democracy and their place within it, in a way that provides insight into democratic national strategic decisions, as well as the degree of successful assimilation of any strategy in accordance with cultural boundaries.

Human progress in the field of technology has led to a connected digital world, which is expressed, among other things, by social media, in ways that link different cultures and facilitate direct and indirect influences. Today, as perceived by the European Union, influence includes the use of information and its disruption by both covert and overt possibilities that often overlap and can be used simultaneously, as illustrated in figure 1 below:

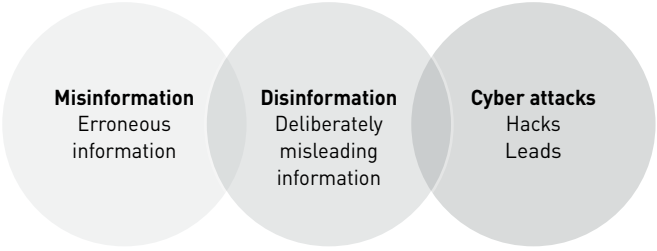

Figure 1: Overlapping Interference
Source: adapted from the European Parliament Research Service, *Council of Europe*, 2017.

Misinformation is defined as information that is incorrect or misleading , but not intentional, while disinformation includes spreading deliberately false information, particularly when supplied by a government.[6]

The Russian information warfare strategy in Europe consists of backing anti-EU parties, acquiring foreign media companies, and supporting extreme political movements. Russia's strategy also involves disseminating disinformation, by spreading half-truths, lies, and conflicting versions of events, in order to confuse and undermine the basis of rational debate. Russia's aim is to strengthen its own image, justify its own actions and policies, and weaken rival narratives, such as Western democracy, the European Union, or NATO, in areas under its influence. Russia operates in this manner throughout

5 Ibid, p. 44.

6 Bentzen, "Foreign Influence Operations in the EU," p. 2.

the year, and not only during elections, although elections are particularly sensitive periods that offer many opportunities to exert influence.[7]

These threats of influence have lead many researchers to attempt to map the ways of coping with them based on various patterns. The model presented by Maria Hellman and Charlotte Wagnsson in their study of threats at the political culture level is useful for the purposes of this article. They examine four coping approaches: confrontation, blocking, naturalizing or reinforcing the national narrative, and ignoring. Their research proposes a series of options that liberal democracies can adopt as a response to information warfare, especially within the context of the Russian operations.[8]

The first approach they consider is confrontation in response to the spreading of opposing narratives. The strategy behind this model includes actively creating counter narratives.[9] For example, an intelligence operation could disseminate information that directly attacks the hostile narrative, as the British General Communications Headquarters (GCHQ) did when they set up a team to create a campaign of counter influence against ISIS. The British cyber department sought to exert internal influence by disseminating the information among local population groups who were at risk of being radicalized by ISIS and by means of external influence by denying services, blocking websites, and interfering with broadcasts to deter individuals or groups.[10]

The naturalizing approach is when a country that is threatened disseminates a positive national narrative of its own. It resembles public diplomacy that is focused solely on the internal context; that is, the country presents itself and its world view in a positive light to foreign audiences and thus gains sympathy without competing with or condemning other narratives.[11]

The blocking approach is a strategy of protecting the national narrative by blocking the narrative of another country. The activity of the country that blocks is defined as being "selective" of the information that is spread by

7 Maria Hellman and Charlotte Wagnsson, "How can European States Respond to Russian Information Warfare? An Analytical Framework," *European Security* 26, no. 2 (2017): 156.

8 Ibid., 154.

9 Ibid., 158.

10 David Bond, "Britain Preparing to Launch New Cyber Warfare Unit," *Financial Time*s, September 21, 2018, https://on.ft.com/2HRkcA0.

11 Hellman and Wagnsson, "How can European States Respond," pp. 159–160.

the rival country; in other words, it prevents public access to information disseminated by the other country by blocking its broadcasting stations or websites.[12]

Ignoring is a strategy of a lack of response to what appears to be a false and manipulative narrative. This model is based on the belief that a strong democracy has sufficient means to cope with external manipulation of information. It should be noted that ignoring does not necessarily mean no response. Rather, the response focuses on strengthening civil society and training professionals in sensitive areas how to critically understand visual and textual media.[13]

While dealing with this challenge, NATO Stratcom realized that interference in elections is a major threat to the democracy of the Western world. It recently published a study that specifically focuses on the advantages of applying a strategic communications mind-set in dealing with the challenges of interference. They see the common stratagems as laundering, point and shriek, flooding, and polarization. Laundering refers to legitimizing false information or altering the origin, mostly known as "fake news." Point and shriek refers to injustices within targeted social groups and heightening emotions among them. Flooding causes confusion by providing contradictory information, and polarization uses deceptive identities to support opposing sides or to lead opinions to greater extremes.[14]

The way they suggest dealing with interference while protecting the elections is by deterring the players through reducing or removing vulnerabilities. Moreover, the establishment of detection and early warning mechanisms is required, with coordination and cooperation for efficient actions, as well as combining education and raising public awareness for further effects.[15]

Four case studies were examined in this research: Sweden, Latvia, Estonia, and Finland. First, the countries were assessed for possible risks to the elections and whether they have established functional mechanisms while expanding responsibilities of state bodies relating to the information sphere. The governments in Latvia and Finland, for example, have educated media organizations as part of the building resilience. Afterwards they built

12 Ibid. p. 161.

13 Ibid, p. 162.

14 NATO Stratcom, "Protecting Elections: A Strategic Communications Approach", June 2019, pp. 9-12, https://bit.ly/2KGYiCE.

15 Ibid., 14.

networks of partners and monitored the information. Raising this subject higher in the political agenda has been the result of applying the Stratcom mindset.[16]

Threats of Influence on the European Countries

The European countries define and perceive the range of threats of influence as mainly various geopolitical points of view and opportunities. Threats of influence, including disinformation, misinformation, and fake news are observed mainly on social media. They find expression through "trolls," referring to users who operate fake accounts and post paid content; and "bots," which are algorithms that disseminate content on social media automatically or semi-automatically and can target specific population segments or groups.[17] The threats of influence are perceived as being mainly foreign, although they may also be internal. Distinguishing between threats is sometimes problematic, artificial, or impossible, because threats often feed on one another, even subconsciously. In Europe, there is broad reference to the Russian threat and its alleged use of information warfare on social media and traditional media, but sometimes the source of the threats actually lies with internal forces and is consciously or unconsciously manipulated by Russia.

The European nations classify the threats by the degree of severity. The Western European countries deal with threats of influence on the democratic process and public belief in the democratic system, its institutions, and its leaders. The Baltic states face threats of influence that could lead to war with Russia, as was the case in the Crimean Peninsula. In contrast, the fledgling democracies that emerged after the collapse of the Soviet Union are worried about Russia's ambitions to take control of strategic areas of their territory.[18]

The regional division used in this article—Baltic states, Nordic states, and the Western European states—can help us to understand the similarities in the nature of the threats. Estonia and Latvia, which share borders with Russia, are at the forefront of the struggle against Russian influence today as well as historically and demonstrate a focused and intense approach for coping with it. A significant part of the Kremlin's influence campaigns are directed at the

16 Ibid., 16-18.

17 Andrew Higgins, "Effort to Expose Russia's 'Troll Army' Draws Vicious Retaliation," *New York Times*, January 19, 2018, https://nyti.ms/2HBWitH.

18 Josh Rubin, "NATO Fears that this Town will be the Epicenter of Conflict with Russia," *The Atlantic*, January 24, 2019, https://bit.ly/2HyUK3x.

Russian-speaking minorities residing in those countries, accounting for 27 percent of the Latvian population and 25 percent of the Estonian population, although the Russian activity is not only targeted at them.[19]

The Baltic states are coping with the threat that the population will divide along ethnic lines so that Russia can establish and maintain its control of the local Russian diaspora—which can serve as a tool for the Kremlin. In addition, Russia is trying to instill among the population in those countries a general mistrust of the governments of the Baltic states, by presenting them as precarious ethnocratic regimes that are facing a rise in fascism. At the same time, Russia's interests are to damage democratic methods in general and particularly the way in which citizens perceive democracy; thus Putin's Russia and its successes is presented as a more stable regime model.

Russia has tried to strategically influence the alliances of the Baltic states with the European Union and NATO, by spreading false information about the citizens of these states or about the soldiers of the forces participating in NATO and the Baltic armies, as the Estonian intelligence service revealed in a report published in 2018.[20] Here Russia presents the Baltic governments as puppets of supra-national organizations that are allegedly trying to push Russia into a military conflict.[21] Moreover, through its media and social networks, Russia actively denies the culture, history, traditions, and achievements of the Baltic states and seeks to strengthen its own status in those countries and prepare the ground for preventing any internal opposition should a military conflict between the Baltic states and Russia occur.[22]

Sweden and Denmark are both test cases for Russian influence in the Nordic states. Since 2014, Russia has been trying in various ways to influence Swedish policy on its cooperation with NATO and the possibility that it will join the alliance, as well as on Sweden's support—as well as

19 Tomas Cizik, "Russia Tailors its Information Warfare to Specific Countries," *European Security Journal*, November 6, 2017, https://bit.ly/2wbruJF.

20 Estonian Foreign Intelligence Service (Välisluureamet), "International Security and Estonia 2018," https://www.valisluureamet.ee/pdf/raport-2018-ENG-web.pdf.

21 Mike Winnerstig, ed., *Tools of Destabilization: Russian Soft Power and Non-Military Influence in the Baltic States* (FOI Swedish Defence Research Agency: December 2014), p. 4.

22 Committee on Foreign Relations United States Senate, "Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security," S. PRT 115–21 (2018), pp. 101f.

of the European Union—to Ukraine following Russia's annexation of the Crimea and the ensuing international criticism.[23] Russia's strategic objective is to reduce NATO's presence in countries that are geographically close to it. In the Swedish case, Russia has disseminated misleading information that sows doubts in the ability of the Swedish political system and tries to incite Swedish society through social media posts that criticize Sweden's acceptance of refugees, as they tried to do in August 2018 just before the Swedish general elections.[24] Denmark, a NATO member, shares with Sweden the geographical link between the Baltic Sea and the North Sea, which is also the shortest sea route between Russia, Europe, and North America.[25] As a result of Russia's annexation of Crimea and Denmark's support for international sanctions against Russia, Denmark is now in a position of needing to cope with increased Russian attempts to influence Danish public opinion and to shift its perceptions of Russia. Denmark's veto on laying a gas pipeline in its territorial waters as part of its Nord Stream 2 project also triggered Russian attempts to influence. According to researchers, Russia would consider any Danish decision to prohibit the pipeline as the result of anti-Russian feeling among the Danish population, which Russia perceives as being nurtured by the United States.[26]

The large Western European countries—Germany, France, and England—are mainly attacked externally by Russia and are targeted because of their central position in the European Union and their status as flag-bearers for liberal values. The broad policy of admitting refugees, particularly of Germany, has led Russia to intensify its efforts to influence its domestic arena. Russia is also helped by the internal ideological crises in these countries, which has strengthened the far right parties and their messages on social media. For example, a spokesman of the right-wing German party "Alternative for Germany" (AfD) claimed that information appearing on social media—even

23 Michael Birnbaum, "Sweden is Taking on Russian Meddling ahead of Fall Elections," *Washington Post*, February 22, 2018, https://wapo.st/2QkVGLB.

24 Anna Knutsson, "Nya narrativ utmanar omvärldens bild av Sverige," *Svenska Institutet*, June 18, 2018, https://bit.ly/2VWmqIc.

25 Alexandr Golts, "The Arctic: A Clash of Interests or Clash of Ambitions," in *Russia in the Arctic*, ed. Stephen J. Blank (Carlisle, PA: The Strategic Studies Institute, US Army War College, 2011), p. 48, https://bit.ly/2HOo5po.

26 Danish Defense Intelligence Service, "Intelligence Risk Assessment 2018," December 21, 2018, p. 21, https://bit.ly/2QjX4y2.

if it was false or incorrect—provided a generally true message, irrespective of its origin.[27] In France, leaks from the social media account of Emanuel Macron during his election to the French presidency, which were published on WikiLeaks, even though some items were false; the incitement against Macron and his activity after his election; and information about the French Police spread during the "Yellow Vests" protests in 2018, which can perhaps also be attributed to external sources, are all examples of the challenges that face these countries.[28]

Germany, France, and England are also coping at various levels with the spread of extreme Muslim ideology and terrorist acts motivated by ISIS propaganda when the organization represented a significant threat to these countries. ISIS's tactic was to exploit ideological, social, economic, and political weaknesses among the target audience in those countries.[29] Moreover, Britain had also been dealing with efforts to influence the referendum on EU membership, which led to Brexit and served the interests of those seeking to weaken the European Union both internally and externally.

Ways of Coping

In the countries mentioned above, we examined the political and governmental methods of handling the threats of influence. These methods include setting up bodies or links between various ministries, educating citizens and senior political figures, and working with the media to combat the dissemination of disinformation and fake news. In addition, we studied the place of civil society in each country within this context. We present the main methods of dealing with the threat and separately discuss the most prominent or unique activities. The methods tend to reflect the approaches that each country adopted, so that the holistic approach represents a balanced combination of approaches; the data security and cyber method represents the confrontational approach, and so on, as discussed in the section connecting approaches to political culture. Several complementary directions of action also took place, some with greater impact, such as educating the public on critical

27 Karolin Schwarz, "Ist Doch Nur Satire?," *CORRECTIV*, September 9, 2017, https://bit.ly/2VMVYvI.

28 "French Yellow Vests, the Far Right, and the Russian Connection," *Tango Noir*, December 12, 2018, https://bit.ly/2wgYxMs.

29 HM Government, "National Security Capability Review," (March 2018), pp. 5–6, https://bit.ly/2HnHafL.

consumption of news, and some with less. It should be noted that the impact of the various efforts is not discussed here.

The Holistic Approach

The holistic approach looks at the system beyond its components and creates a broad, inclusive overview. One country that uses the holistic approach to tackle the challenge of influence and combines a number of courses of action into an organized national policy is Denmark, which is highly aware of external efforts, mainly by Russia, to influence it. According to Defense Minister Claus Hjort Frederiksen, within Denmark, it is possible to identify the Russian "propaganda designed to improve the image of Russia and its activities, and undermine our belief in ourselves."[30]

In September 2017, Denmark set up an inter-ministerial body to strengthen cooperation between the various ministries of defense and justice as well as intelligence and national security agencies and to coordinate activities inside and outside the government in order to address the threat of influence. A year later, the government published its "Eleven-Step Plan," designed to provide steps to reinforce Danish opposition to attempts to influence.[31] The next stage has been to strengthen the monitoring of disinformation in the country by training people in the media, while supporting the efforts of the Danish Security Service and Defense Intelligence to respond to campaigns of influence. This approach led to energetic organizing in order to cope with the efforts of external influence in the period leading up to the Danish elections in 2019. As part of the efforts to deal with the threat, assessments of threats and risks were published, as a result of cooperation between Danish intelligence bodies, the Ministry of Economy, and Ministry of Internal Security, while national preparedness to deal with external campaigns prior to the elections reached emergency levels. The government also announced that it intended to advise the various political parties and their leaders on the threats and how to handle them. It stressed the importance of dialogue and cooperation with the media, including full respect for the core principles of press freedom and independence. At the same time, Danish legislation

30 "Denmark to Educate Soldiers in Combatting Disinformation," *EU vs Disinformation*, August 23, 2017, https://bit.ly/2M2YuhX.

31 "Strengthened Safeguards against Foreign Influence on Danish Elections and Democracy," *Ministry of Foreign Affairs of Denmark*, https://bit.ly/2U0aHmR.

on foreign influence was amended, while the government also took steps to raise awareness of these threats among the population.[32]

Data Security and Cyber Protection

This approach centers around the identification, exposure, and blocking of information warfare through data security and cyber protection. It involves political-security activities by civil society organizations, as well as private companies. This approach is characteristic of the confrontational approach, which sets up a counternarrative to influence efforts and actively fights them. The importance of data security is based in the understanding that leaks of genuine information are central to the threat of influence, in which the targets of attack are not necessarily security-related but rather political parties and politicians.

Britain is a leader in using the confrontational policy, due to its experience in dealing with extreme ideological influences and external interference in its EU membership referendum. It combines a political and civilian approach and includes a broad cybersecurity strategy formulated by the National Cyber Security Center (NCSC). As a result of this strategy, political parties were warned of the risk of Russian hackers and attempts to influence social media. The NCSC cooperates with individuals, companies, and organizations by "sharing information about cybersecurity."[33] In addition, the Government Communications Service (GCS) published a toolkit called RESIST intended to aid media people in handling the threat of disinformation. It includes training on how to identify a wide range of fake news items, prevent their dissemination, and—unlike other guides—how to develop a response. Disinformation affects the work of organizations as well as the general public, and the response is based on both short-term and long-term strategic communication. For example, if the disinformation requires an immediate response, the toolkit suggests to distribute a counter narrative, or a fact-based correction in the traditional media and on social media. On the other hand, misleading information also requires a more coherent, ongoing response of disseminating a strategic narrative in the information space.[34]

32 Ibid.

33 William James, "UK Political Parties Warned of Russian Hacking Threat: Report," *Reuters*, March 12, 2017, https://reut.rs/2JZJhf1.

34 Government Communication Service, "RESIST: Counter-Disinformation Toolkit," (2019), https://gcs.civilservice.gov.uk/guidance/resist-counter-disinformation-toolkit/.

Many countries strengthen their defenses against cyber threats using this approach. For example, Latvia set up the National Computer Security Incident Response Team (CERT.LV), which works with the government cyber authority and includes over 600 IT experts from government institutions and local authorities. This cooperation yields cyber protection and warnings and includes workshops to raise awareness on the subjects of influence and disinformation.[35]

Educating the Public

Teaching the public to take a critical approach, raise doubts about information on social media and other media outlets, check sources, dates, and so on, are all means of dealing with the threats as part of the method of ignoring them. As part of strengthening democracy, the state and civil society can educate the public in this method, which enables ordinary citizens to distinguish attempts to influence them and handle them without having to confront the hostile narrative.

This method of handling the threat by educating the public is most common in Sweden and is apparent both in government policy and in civil society activity. The Swedish government works through a unit in the Ministry of Defense, called the MSB (the Civil Contingencies Agency). The MSB focuses on public awareness, and prior to the elections, it educated senior figures and government bodies, including the Central Elections Authority and the police, on the need to be prepared for possible interference and influence on the elections process and for developing the ability to identify weaknesses in the system. In reference to Swedish policy, which champions the idea of not using fire to respond to fire, the head of global monitoring and analysis in the MSB, Mikael Tofvesson said that "it's like fighting with a pig in mud. You both get dirty, but the pig will think it's quite nice."[36] As a result, Sweden chooses to focus on democracy and freedom of expression by providing the public with correct information as the best means of defense. The Swedish Institute, a public institute that promotes interest and trust in Sweden, has developed a detailed educational program called Fake ≠ Fact,

35 Ģederts Ģelzis, "Latvia Launches Cyber Defence Unit to Beef up Online Security," *Deutsche Welle*, March 4, 2014, https://bit.ly/2wbOoR2.

36 Emma Löfgren, "How Sweden's Getting Ready for the Election-year Information War," *The Local*, November 7, 2017, https://bit.ly/2KULjyr.

which can be freely downloaded and is intended to provide teachers with the tools for teaching critical thinking to the younger generation and thus protect Swedish society from false information and propaganda.[37]

Another country that invests in educating the public is France. Entre Les Lignes ("Between the Lines") is an organization of a hundred journalists, photographers, and volunteers from the French media who give workshops designed to encourage pupils to be wary of the sources of information reaching them, particularly on the internet.[38]

A study by IREX, an organization that specializes in development and in global education, examined the effectiveness of educating the younger generation as a means of dealing with influencing specifically in Ukraine. Although Ukraine is not included in the research for this paper, IREX's study showed the ability of pupils in eighth and ninth grade to identify false information after taking lessons on techniques of media literacy led by the organization. Following the training, pupils were able to identify twice as many hate messages and could identify 18 percent more fake news than pupils who did not receive the training.[39]

Coping Through Research

Research institutes, universities, and colleges all are engaging in research on attempts to influence and different means of coping. The research can be divided into theoretical research and research on public discourse. Theoretical research focuses on illustrating and explaining terms and analyzing test cases, while the research on the public discourse analyzes public opinion, as expressed mainly on social media, in order to identify efforts to disrupt and interfere. This research could help to reinforce the national narrative by creating explanations for hostile narratives, facilitating the presentation of a social-academic narrative of progress, and strengthening the public's knowledge and its faith in the truth.

Stratcom is a NATO research institute in Riga, Latvia. It combines theoretical and operative research in order to achieve a better comprehend the challenges, the limits of influence through social media, and to understand

37 "Fake ≠ Fact," *Sharing Sweden*, December 2017, https://bit.ly/2weRmEe.

38 Entre les Lignes: Association D'Éducation aux Medias et a L'information, *Entre les Lignes,* 2019, https://bit.ly/2EsfWpL.

39 Sasha Ingber, "Students in Ukraine Learn How to Spot Fake Stories, Propaganda and Hate Speech," *NPR*, March 22, 2019, https://n.pr/2HOlKLj.

Russian activity in Europe. The Baltic Center for Media Excellence is prominent for its work in identifying fake news and propaganda. The center also operates as an advisory body and develops workshops on dealing with disinformation and fake news and education for critical thinking.[40] Other research institutes, such as the Danish Institute for International Studies, mainly focus on theoretical studies of foreign intervention and disinformation. At the same time, the Danish Institute also engages in research on how to deal with such intervention and disinformation and presents its findings and means of identifying these activities on social media, particularly to high school students. Copenhagen University also deals with these issues, focusing on inter-disciplinary research on digital information warfare and the function of public debate.[41]

Civil society in the United Kingdom demonstrates a similar line of action, by looking at the discourse, while the universities tend to focus on internet research. Edinburgh University, for example studies the activities of Russian bots. These studies have exposed attempts to exert influence on the referendum on EU membership ("Brexit").[42] The independent Institute for Statecraft also researches Russian attempts to influence as well as the war on disinformation.

Restricting Attempts to Influence

The approach of blocking attempts to influence is manifested by restrictions on broadcasting channels, websites, users, or content. These steps are widely accepted in the Baltic states of Estonia and Latvia, although other countries also engage in similar restrictions, albeit at a lower level and more focused. Some countries adopt this approach as a result of the position of the social media companies in their countries. In discussions on disinformation and influence, various governments in Europe and the European Union have stressed the responsibility of companies, such as Facebook, Twitter, YouTube, and Google for allowing the misleading, inciteful, or fake information.[43]

---

40 "Our Mission," *Baltic Center for Media Excellence*, 2019, https://bit.ly/2WZteBf.

41 "Exploring Digital Disinformation and its Effects in the 21st Century," *Digital Disinformation – Department of Political Science*, https://disinfo.ku.dk/.

42 Matthew Weaver et al., "Russia Used Hundreds of Fake Accounts to Tweet about Brexit, Data Shows," *Guardian*, November 14, 2017, https://bit.ly/2K17b9F.

43 "Facebook, Twitter doing too Little against Disinformation: EU," *Phys*, February 28, 2019, https://bit.ly/2YDg8Ku.

The main way of dealing with the problem is by adapting the algorithms of these platforms to identify and stop the spread of misleading posts and by activating automatic tools to identify automated activity or activity that breaches community rules. For example, the community rules on Facebook prohibit users from having more than one profile, and therefore each "bot" or paid fake user is in breach of the terms.

Estonia and Latvia made a strategic decision to limit content published outside of social media. Thus, these countries supervise Russian media channels, impose fines for incitement, and sometimes even block the channels on accusations of having breached local media laws.[44] Estonia has even created a media alternative, which broadens the struggle against the hostile narrative. In 2015, a public Russian-language TV channel was established in Estonia, which broadcasts claims that counter pro-Russian broadcasts and thus reduces the gap and the alienation felt by the country's Russian-speaking population.[45]

Political Responses to Efforts to Influence

The response of the political system and politicians—whether by raising public awareness or by training senior figures (as seen in one of the Danish initiatives)—is an important dimension of the struggle against efforts to influence. Public statements made by political leaders represent the confrontational approach, as they publicly present the hostile narrative and its purpose, sometimes with a warning against these attempts to intervene. For example, Foreign Minister Edgar Rinkēvičs of Latvia often warns against outside influence, as does the president of Estonia, who even stresses Russia's role in the activity.[46] France's President Emanuel Macron is known for his statements against fake news and disinformation, as is Britain's Prime Minister Theresa May, who turned directly to Russia during the parliamentary elections and stated bluntly, "We know what you're doing, and it won't succeed," in reference to Russia's use of digital warfare.[47]

---

44 "Fighting Disinformation in the Baltic States," *Foreign Policy Research Institute*, July 6, 2017, https://bit.ly/2JCEnoP.

45 Ibid.

46 Lally Weymouth, "'Russia Is a Threat': Estonia Frets about Its Neighbor," *Washington Post*, March 24, 2017, https://wapo.st/2EseSCq.

47 Jon Craig, "PM warns Putin: We Know What You're Doing and It Won't Succeed," *Sky News*, November 14, 2017, https://bit.ly/2zWlsAB.

In addition to making public statements, public figures also take their own steps to fight the challenges of influencing. For example, Estonian public figures have announced that they refuse to be interviewed for Russian state media because "there is no reason to give interviews, when the story has already been written."[48] In this manner, they sought to undermine the legitimacy of Russian media and the trust in it. Similarly, in Germany, party leaders (excluding the right-wing AfD) signed a "gentlemen's agreement" before the elections, in which they promised not to use bots on social media, an agreement that was indeed honored.[49]

Legislation

Legislation and regulations are tools that reflect responsibility of the state as being at the center of the struggle to curb influence. Researchers consider this as similar to blocking, since it limits certain activities and may encounter criticism. Germany leads in this kind of legislation. In 2017, it passed the Network Enforcement Act, designed to combat the spread of fake news and hate speech via the internet. In an unusual step for Western democracies, the law stated that networks such as Facebook and Twitter must remove fake news items that encourage hatred or that have "criminal" content within 24 hours after posting, otherwise they could face fines of fifty million euros. So far no actual fines have been reported. The UN condemned the German law saying it bordered on censorship and damaged freedom of the press.[50]

In July 2018, France, which has faced attempts to influence its presidential elections, passed a law against the dissemination of fake news, particularly during elections. The law states that if fake news is published during an election campaign, the legal authorities will be able to block content or the site where the content appears. The law also demands greater transparency regarding sources of funding for websites.[51]

---

48 "Estonia's Lessons for Fighting Russian Disinformation," *Christian Science Monitor*, March 24, 2017, https://bit.ly/2qJKg8s.

49 *Make Germany Great Again – Kremlin, Alt-Right and International Influences in the 2017 German Elections* (London: Institute for Strategic Dialogue, 2017), pp. 12–13.

50 Erik Brattberg and Tim Maurer, *Russia's Elections Interference: Europe's Counter to Fake News and Cyber Attacks* (Washington DC: Carnegie Endowment for International Peace, May 2018), p. 20.

51 Michael Ross Fiorentino, "France Passes Controversial 'Fake News' Law," *Euronews*, November 22, 2018, https://bit.ly/2FBn0U7.

Checking the Facts

Fact-checking websites are another expression of how civil society deals with false information and attempts to influence. While the impact of this method is not great, as it is a narrowly focused response to information that has already been published, it does present an active debate on the truth and options for internal cooperation. For example, in France, sixteen different journals, including *Le Monde*, *Google NewsLab*, and *First Draft*, cooperate to check facts. The project is called CrossCheck and it focuses mainly on election campaigns, with the purpose of informing the public about the information needed. It does this by sharing with the public its opinions and news items in real time. This cooperation encourages exchange of ideas while fact-checking, at the expense of the competition between the journals.[52] Another example is the independent German blog called BildBlog, which focuses on verifying information and video clips on social media. The activity of those who report on this blog about false news items increases the public's awareness about disinformation and encourages cautious attitude to the flow of information.

Between Political Culture and Approaches to Coping

It is possible to map how countries address the problem of foreign influence by analyzing their different approaches in regards to their political culture. Gary Schaub, a researcher from the Center for Military Studies at Copenhagen University, argues that Russia's disinformation does not have much effect in Denmark as it does elsewhere because of the Danish political culture. According to Schaub, "The difficulty derives from the Scandinavian culture, that builds consensus and social robustness, which are an obstacle to attempts at influence."[53]

Both Estonia and Latvia have a similar political culture, having emerged as fledgling democracies after the fall of the Soviet Union. Their perception of democracy is intertwined with notions of unity and preserving their democratic principles and its basic fundamentals, and not of promoting advanced values as in the West, together with the shaky progress of civil society and its efforts

52 "CrossCheck – a Collaborative Journalism Project," *First Draft,* https://firstdraftnews.org/project/crosscheck/.

53 Robbin Laird, "Shaping a Way Ahead in Nordic Defense," *Second Line of Defense*, October 15, 2017, https://bit.ly/2X1O4jH.

against the values of the institutional political system.[54] Both countries have demonstrated a pattern of strategic choices that champion the blocking approach. As already mentioned above, for example, Estonia established a Russian-language television channel whose purpose is to publish counter narratives to the Russian ones, thus constructing a unique Estonian narrative. Similarly, Lithuania, the neighbor of Estonia and Latvia, also has sought to block the Russian TV channel, RT. The blocking approach is not suitable for countries that have a political culture based on a progressive and developed liberal concept of democracy and its values, as it could be perceived by the public in those countries as "cultural imperialism" or censorship. However, fledgling democracies, such as the Baltic states, recognize its importance as they seek to defend themselves with various methods, including blocking.[55]

Since 1990, Germany has shaped a political culture whose main purpose has been to unite East and West Germany. Combining the different political cultures of West and East Germany, this process required a high degree of commitment to basic democratic values and tolerance based on Germany's previous historical experience. Nevertheless, research indicates that the political culture of the two parts of Germany are still different, with eastern Germany having less faith in democracy than the western part.[56] Thus, it becomes clear that in its current way of coping with the challenge of external influence, Germany prefers to reinforce the German narrative and chooses options that increase transparency on the internet. The choice to emphasize its national narrative is strengthened by Germany's political and cultural leadership in the European Union and by its having a history of acknowledging its internal narratives and understanding their power and significance. This understanding has led Germany to block the spread of narratives that it deems threatening as well as to pass legislation imposing fines on social media for the spread of fake news.

The Nordic countries are characterized by a culture of self-criticism in the fields of society, politics, and economics. This criticism reflects an open political culture that believes in democracy and the power of the people,

54 Martin Stefek, "Post-Communist Central East European Political Culture in the Era of Neoliberalism," *Delhi Business Review* 14, no. 1 (2013): 25.

55 Hellman and Wagnsson, "How can European States Respond to Russian Information Warfare?," p. 161.

56 Russell J. Dalton and Steven Weldon, "Germans Divided? Political Culture in a United Germany," *German Politics* 19, no. 1 (2010): 9–23.

based on the perception that participatory democracy is a progressive and rational project. This perception means that education occupies an elevated position in Nordic cultural values.[57] Thus, it is possible to understand, for example, why Sweden generally chooses the strategy to ignore the efforts to influence. This choice emanates mainly from a belief in democratic institutions and their power and in the belief that non-intervention and the maintenance of open dialogue strengthen the credibility of these institutions in society.[58]At the same time, depending upon the ability of citizens to deal with foreign narratives could ultimately become a weakness, particularly when Sweden relies on the traditional media as an objective player in the defense of democracy. For example, when external efforts to exert influence cross the boundaries of the internet in Sweden, the state takes steps to strengthen the local narrative, as it did in the media coverage of a joint Sweden-NATO military exercise.[59] The special relationship between Sweden and NATO is a target for Russian efforts, and when they attack the positive narrative that Sweden tries to portray, this only reinforces Sweden's interest in projecting internally positive narratives.

Britain, whose political culture was the subject of a study by Gabriel Almond and which is still relevant today, has a dynamic political culture based on its status as an island, rich in history and wars, and as a democracy that has progressed by evolution rather than revolution.[60] Britain leads the confrontational approach, choosing an operative strategy that invests in spreading counter narratives to hostile ones. This approach suits Britain's political culture, which believes in its ability to lead the international system and in its importance vis-à-vis both the United States and Europe. While British democracy faces threats from several directions, it tries to define its narrative in an era of internal political change. In particular, this is the case given the choice to leave the European Union on one hand, and internal opposition to the results of the referendum that followed, on the other hand.

57 Ainur Elmgren and Norbert Götze, "'Power Investigation: The Political Culture of Nordic Self-Understanding': Introduction," *Journal of Contemporary European Studies* 21, no. 3 (2013): 338–340.

58 Ibid, p. 162.

59 Reuters, "Fears of Russia: Sweden Starts a Military Exercise with NATO Support," *Ynet*, September 14, 2017 [in Hebrew], https://bit.ly/2VZATTW.

60 Gabriel Almond and Sidney Verba, *The Civic Culture* (Boston: Little, Brown, 1965).

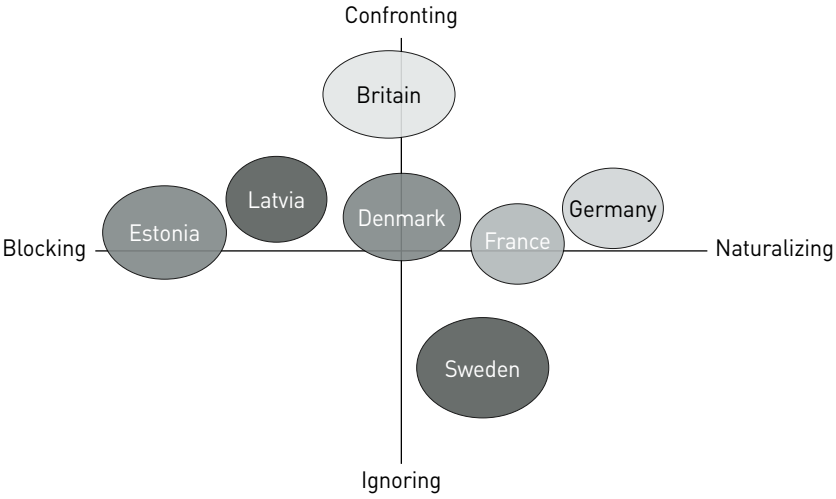

Figure 2: Choice of Approaches

Figure 2 above shows a possible distribution of the seven countries examined in this article and their modes of dealing with foreign influence. The graphic presentation shows the proximity of the countries to the various approaches. Thus, Denmark is at the center in order to illustrate its holistic approach, which integrates the various approaches. The propinquity of the countries can be explained by their political culture and the choice of the strategic narrative of each country, its citizens, and history. By looking at the picture as a whole, we can examine the various means used to deal with the threat and the possibility of adopting them in other countries, including Israel.

Conclusion

The different ways of dealing with the challenge of influence as presented here suggests several conclusions. Cooperation between the government, political parties, politicians, the intelligence and security communities, media companies, and civil society is needed so that each country can address the threat. Denmark is a good example of such cooperation, but other forms of cooperation also can contribute to managing this phenomenon.

In each country studied, the perception of the threat differs, even though the threats are similar (originating in Russia) and this affects each country's chosen strategies. For example, Sweden does not perceive Russia's attempts to undermine the European Union as a threat that requires a counternarrative,

unlike Germany, which puts the European Union and its values at the forefront of its national priorities. This is part of the definition of the strategic importance of narratives and the willingness of civil society to cooperate according to the limits of democracy and its values.

This article presents one possible way of analyzing how European countries are facing the challenge of foreign influence and discusses the main approaches and reasons for each country's choice of approach, shaped by the political culture of each—the British confrontational approach to Russia; Sweden's ignoring of Russia, Estonia's decision to block Russian influence, and the reinforcing or naturalizing of the national narrative in Germany. The different countries create strategies that combine approaches based on their historical experience and how their societies perceive themselves and their democracy.

Further research on this subject is essential, in order to expand its scope beyond these countries and beyond Europe. Other countries in Europe have different ways of handling the threat of influence, which is not necessarily due to an absence of threats. Countries on other continents also have their own way of approaching the challenges, which can be linked to their own political cultures. For example, Nigeria is trying to deal with attempts to influence its election campaign, while New Zealand must face polluting the local dialogue following the massacres in the mosques in March 2018. Further research should emphasize coping methods that are not necessarily related to election campaigns, although these are periods when it is particularly easy to influence viewpoints.

Israeli society, especially during elections, faces both internal and external threats of influence that challenge the stability of its democracy, its institutions, and undermine trust in them. Shared government and citizen efforts, as well as learning from western countries that have already prepared for similar threats, could help Israel formulate a national response to existing or potential attempts of external influence. Further research could focus on Israel's political culture in order to suggest possible responses to the threats of foreign influence, based on Israel's perception of the threats. Political culture in Israel, based on its values, norms, and its unique, complex history, reveals a people who combine critical views of the government with a loyalty

and willingness to participate in politics.[61] An approach that combines the efforts of both government and enterprising civil society in Israel with the importance of confronting the narratives reinforced with education and a blocking approach that utilizes Israel's advantages in cyberspace, if possible, will create a model that increases national robustness in the face of foreign efforts to influence events. Such a model would be especially effective in a society as full of rifts and opportunities as Israel.

61 Yoav Peled and Gershon Shafir, "From a Dialogue on Pioneering to a Dialogue on Rights: Identity and Citizenship in Israel," in *Society in the Mirror*, ed. Hanna Herzog (Tel Aviv: Ramot, 2000), p. 520.

The Threat of Foreign Interference in the 2019 Elections in Israel and Ways of Handling it

Pnina Shuker and Gabi Siboni

In recent years, foreign countries has increased their attempts to influence democratic processes in rival countries. The aim is to damage the electoral process via cyberattacks on computerized systems or to try and affect the outcomes. Examining the electoral process in Israel makes it possible to identify such attempts and propose ways of dealing with them. This article suggests the need to distinguish between foreign attempts to influence the elections and domestic ones, which are part of the democratic process, and outlines directions for action to improve efforts to counter foreign interference in the elections.

Keywords: Elections, influence, cyber, democratic process, social media

Introduction

The possibility that a foreign country would try to influence the democratic process in Israel sparked intensive activity leading up to the elections to the twenty-first Knesset. In July 2017, Lt. Gen. Gadi Eisenkot, then the chief of staff, raised the possibility of foreign interference in Israel's democracy, which he described as a vital challenge. In a debate in the Knesset, Eisenkot

Pnina Shuker is a Neubauer research associate at INSS and a doctoral student in the Political Science Department at Bar Ilan University. Prof. Gabi Siboni is the director of the Cyber Security Program at INSS.

mentioned two related phenomena: attempts to interfere with the outcome of the elections by hacking into and damaging the computer-support systems and attempts to influence voters through mass manipulation, by means of posts and ads on social media and internet sites.[1]

Following the announcement that the elections would be brought forward to 2019, senior political and defense figures in Israel expressed many warnings about possible foreign interference. In December 2018, at the Dov Lautman Conference on Educational Policy, Israel's President Rivlin said that "interested parties want to divert attention from the facts to speculation and defamation . . . In the world of 'fake news' we must safeguard the right of citizens to have access to facts without distortion."[2] The president did not clarify whether he was referring to foreign interference or to the political debate within the country. In early January 2019, the head of the General Security Services (GSS), Nadav Argaman, warned that a foreign country was planning to intervene in the elections in Israel, and that the attack could be cyber-based.[3] At the end of that month, at the Cybertech Conference, Prime Minister Netanyahu also declared that Iran was trying to sway the elections in Israel by means of fake network accounts, and it was conducting cyberattacks against Israel "on a daily basis."[4] According to State Comptroller Yosef Shapiro, "foreign intervention that damages the reliability of the systems and of the results would have a drastic effect on public trust in the authorities."[5]

These statements reflected the considerable anxiety among senior politicians and military/security personnel in Israel over the possibility of foreign interference in the Knesset elections, which, for the first time in the state's history, were held in the shadow of this fear. Given this background, this article examines the danger of foreign interference in the 2019 elections and the efforts to address the threat. This article does not consider attempts to

1 Amos Harel, "The Cyber Authority Prepares a Plan of Defense against Foreign Interference in Israel's Elections, *Haaretz*, July 13, 2017.

2 "State President at Dov Lautman Conference: 'Change from Identity Politics to Ideas Politics,'" *Ynet,* December 27, 2018.

3 Amir Buchbut and Yaki Adamker, "Head of the GSS Warns: A Foreign Country is Planning to Interfere in the Elections in Israel," *Walla*, January 8, 2019.

4 Itai Shickman, "Iranian Cyberattacks are Constantly Monitored," *Ynet*, January 29, 2019.

5 Buchbut and Adamker, "Head of the GSS Warns."

influence and manipulate perceptions within the framework of the political and democratic debate within Israel, which are part of Israel's freedom of expression and which Israeli democracy can and should accept.

The first part of the article surveys the phenomenon and characteristics of foreign interference in elections globally across electoral systems. The second part describes the ways in which Israel has prepared to deal with this problem. Finally, the article examines ways of improving how Israel handles similar challenges.

The Phenomenon of Foreign Interference in Democratic Elections

In recent years, foreign elements (governments and non-governmental) have used digital techniques to damage the democratic process in rival countries. They engage in cyberattacks on computerized systems supporting the electoral process in those countries (databases, software, communications systems) in order to damage or steal data, or to interfere with the operating of these systems. In addition, various methods involving large-scale campaigns to subliminally influence voters have also been exposed. These attempts have a range of objectives, from undermining public faith in the democratic process to affecting the support for specific parties and candidates. Sometimes the goal is to dissuade people from participating in the elections on their basis of their identity or socioeconomic status.[6] These efforts have made extensive use of social media.

Contrary to the perception that social media exposes people to a wide variety of views and opinions, it is clear that Facebook—the most popular social network—actually creates closed spaces of users with homogenous views. These closed spaces occur as a result of users' actions, such as blocking friends or removing them from the list of followers, or attacking anyone who expresses different political opinions, particularly in the case of network members whose links are weak. Thus, Facebook can create separation, even polarization and extremism, in the case of political views, instead of encouraging moderation and tolerance of a wide range of opinions.

6 Chris Tenove, Joran Buffie, Spencer McKay, and David Moscrop, *Digital Threats to Democratic Elections: How Foreign Actors Use Digital Techniques to Undermine Democracy* (Vancouver: Center for the Study of Democratic Institutions, University of British Columbia, 2018), p. 26.

In addition, the network's software, which, among other things, collects data about users and their friends' lists, shares specific information with each user based on their personal preferences. This is another factor contributing to a homogenous social environment,[7] due to the human tendency to connect with others who share similarities—ethnic, geographic, ideological—a phenomenon known as homophilia. This tendency, leading to the "herd" mentality on social media, is reinforced by the social media search engines, which generate results that match the user's attitudes.

The problem is that many people still regard what they see on the internet as a true representation of world events, even though it is, in fact, a subjective display tailored to the user and the user's location, economic and social status, relationships and so on. In the context of the elections in Israel, Karine Nahon notes that, in the elections to the twentieth Knesset, many left-wing internet users assumed that the left would win the elections, on the basis of what they saw on Facebook. The flow of information has extensive influence, so that if we examine this case, for example, the assumption that "the left is going to win" could perhaps cause some left-wing voters not to bother voting, since "in any case we're winning."[8]

Efforts to manipulate public opinion or to distribute information on networks are carried out partly by "bots." A bot, short for robot, is a software agent designed for a range of uses. The principle use in this context is the creation of user profiles on social media or software tools to increase the spread of specific posts. Sometimes, the software is able to handle a large number of entities simultaneously. In this way it is possible to distribute a wide range of content aimed at specific interests—commercial, political, or criminal—with the potential for various kinds of abuse, but the common denominator is the use of automation technologies to influence the flow and spread of information.[9]

It is possible to create and distribute disinformation that is focused on reinforcing existing controversies, such as conflicts between parties, in order

7 Nicholas A. John and Shira Dvir-Gvirsman, "'I Don't Like You Any More': Facebook Unfriending by Israelis During the Israel–Gaza Conflict of 2014," *Journal of Communication* 65, no. 6 (2010): 953–974.

8 Roi Goldschmidt, "Distributing False Information on the Internet and Cyberattacks Intended to Influence Elections," Knesset Research & Information Center, June 2017 [in Hebrew].

9 Ibid.

to drive a wedge between allies and undermine shared norms of democratic debate. For example, Russia used social media platforms in the 2016 US presidential elections, spreading messages that purported to show Muslim support of Hillary Clinton. In this context, they purchased advertising space on Facebook where they ran messages such as "Support Hillary; save American Muslims." The purpose was to link political Islam to Clinton.[10] In addition, there was a great deal of activity intended to encourage black Americans to participate in demonstrations and disrupt public order.[11]

Disinformation can also be used to deter people from participating in polls. Research on elections shows that election posters only occasionally seek to persuade people to change their voting intentions, and that they can be more effective in raising or lowering voting rates and influencing the vote in favor of less well-known candidates. In addition, it is possible to harm democratic participation by using digital techniques in order to extort, threaten, or harass candidates.[12]

According to Karine Nahon, the problem of erroneous or distorted information is particularly troublesome during events such as war or elections where the demand for information is greater than usual, and the media tends to spread information quickly, often without sufficient, in-depth fact checking. As a result, the public do not "check the facts" but rather adopt positions based on false information, or when beliefs that they already hold are reinforced. Nahon states that social media and viral items on the internet provide much greater possibilities for using disinformation as a means of influencing people during elections.[13]

To sum up, the ability to vote and influence—the most basic form of political participation—is currently under threat from foreign digital interference. As stated above, this interference can be achieved through cyberattacks on

10 David Siman Tov and Yotam Rosner, "Conscious Undermining: Russia in the US Presidential elections as a New Threat to the West," *INSS Insight* no.1031 (Tel Aviv: Institute for National Security Studies), March 8, 2018.

11 Leonid Nevezlin, "The World's Most Dangerous Troll," *Liberal,* February 2019 [in Hebrew].

12 Tenove and others, *Digital Threats to Democratic Elections*.

13 Goldschmidt, "Distributing False Information on the Internet and Cyberattacks in Order to Influence Elections."

computerized-support systems in order to disrupt *the electoral process*, or through disinformation campaigns intended to affect *the election results*.[14]

Attempts to Influence Elections Worldwide

In recent years, there have been numerous cases of countries intervening in the electoral processes of other countries using internet-based technology. Over the last decade, Russia has been particularly prominent (although it is not alone) among the countries that have used cyber means to influence elections. It attempted to interfere in the elections in Ukraine (2014), in the United States (2016), France, Germany and Holland (2017), and in referenda in Britain, Holland, Italy, and Spain (2017).[15]

The most striking recent example of interference in elections, whose results continue to affect the United States as well as the entire world, is the case of Russian intervention in the US presidential elections in 2016. In early January 2017, the American intelligence community published its assessment that Russia had interfered in the elections using a range of means in order to damage the chances of the Democratic candidate Hillary Clinton and promote the election of Donald Trump.[16] The report states that Russia's efforts included cyber campaigns on social media, in which they used bots, trolls, and hackers to simultaneously spread disinformation regarding a number of competing narratives, in order to exacerbate existing conflicts within American society and undermine trust in western institutions and the democratic process in general.[17]

In February and July 2017, Special Prosecutor Robert Mueller submitted detailed indictments against twenty Russian citizens for interference in the US presidential elections. Nevertheless, no clear explanation has been given of how this interference actually affected the election campaign or the outcome. Even the most prominent research on this subject does not state unequivocally that Russian attempts to exert influence bore fruit but rather

14 Tenove and others, *Digital Threats to Democratic Elections.*

15 Eli Bechar and Ron Shamir, "Cyber Attacks on Electoral Systems: How to Deal with Them?," *Policy Research* (Jerusalem: Israeli Institute for Democracy and Research Program on Cyber Defense) 136 (2019): 9–10 [in Hebrew].

16 Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections," January 2017.

17 Andrew Radin and Elina Treyger, "Countering Russian Social Media Influence," *RAND Corporation*, November 2018.

assumes that this is highly probable, based on the circumstantial overlap between Russian efforts and changes in the public and media debate and the surprising results of the elections.[18] It is worth noting that at the end of March 2019, Mueller published his final conclusions, which, in fact, confirmed the conclusions of the Senate Intelligence Committee report of 2017, that Russia had conducted a campaign of hacking into computer systems and spreading disinformation designed to deepen rifts in American society and influence the 2016 elections. Mueller identified two arms of the Kremlin's campaign: the dissemination of false information run by an organization known as the Internet Research Agency and hacking of computer systems by Russian intelligence bodies that worked against the Democratic party.[19]

It is clear, however, that not only Russia has interfered in democratic elections. China did the same in the 2018 elections in Cambodia,[20] while an increasing number of reports have pointed to Chinese efforts to interfere in the US elections, which led President Trump to announce that China was seeking to influence the November 2018 mid-term elections to the US Congress and other institutions.[21] At the end of January 2019, Facebook and Twitter both announced that they had exposed an Iranian secret attempt to exert cyber influence on Israel. It included content that was designed to reinforce the Iranian narrative regarding developments in the Middle East and on the Israel-Palestine conflict, as well as criticism of Prime Minister Netanyahu, his policy, and his family, apparently in an attempt to sway Israeli public opinion before the Knesset elections. The link, however, is circumstantial and it is not clear whether the moves attributed to Iran were indeed intended to affect the elections in Israel.[22]

---

18 Kathleen Hall Jamieson, *Cyber-War: How Russian Hackers and Trolls Helped Elect a President* (Oxford: Oxford University Press, 2018).

19 US Department of Justice, Special Counsel Robert S. Mueller, "Report on the Investigation into Russian Interference in the 2016 Presidential Election," March 2019.

20 Scott Henderson, Steve Miller, Dan Perez, Marcin Siedlarz, Ben Wilson, and Ben Read, "Chinese Espionage Group TEMP.Periscope Targets Cambodia Ahead of July 2018 Elections and Reveals Broad Operations Globally," *FireEye*, July 10, 2018.

21 Abigail Grace, "China's Influence Operations are Pinpointing America's Weaknesses," *FP*, October 4, 2018.

22 Hagar Buchbut, "Facebook Removes Hundreds of Pages Containing Iranian Fake News," *Ynet,* January 31, 2019 [in Hebrew].

At the time of writing, it is not clear to what extent the 2019 elections in Israel were a target for foreign interference and to what degree (if at all) such interference succeeded. Whatever the case, the State of Israel implemented protective efforts before and during the elections.

Efforts to Protect against Foreign Intervention in the 2019 Israeli Elections

There are three possible types of cyberattacks in the context of the Israeli elections. The first is the "classic" cyberattack designed to interfere with the electoral system and the democratic process, including attacks on computerized systems and databases that support the electoral process, or that are related to political parties and polling companies.[23] The second is an attack on political parties and candidates in various ways, such as theft of personal and political data to be published at the most damaging opportunity, disruption of party preparations for the elections, and more. The third includes attempts to subliminally influence public opinion through social media.

Responding to these threats is a complex challenge, and it is important to distinguish between efforts by political parties themselves—a legitimate process that every democratic society must allow—and efforts by foreign elements. Any response may involve an infringement of privacy as a result of monitoring social media. The "classic" cyber threat requires defensive efforts by the interested parties, such as the Central Election Committee (CEC), the parties, polling companies, and other elements that could be exposed to these attacks. The National Cyber Directorate (NCD) has undertaken to provide assistance to all relevant bodies and is working with the Central Election Committee to combat the threat.

National preparations for the elections to the twenty-first Knesset included the establishment of a special elections team led by the NCD, with members from the defense establishment and the Ministry of Justice. The team met regularly, and its activities were based on learning from the experiences of other countries and carrying out exercises with the relevant bodies—the CEC and others in the political and civil systems (such as polling companies). This signified a substantial advance in national readiness in dealing with threats to the democratic process, although at this stage it is only in the context of

23 This is in contrast to efforts to influence the outcomes by means of activity on social media or harmful revelations about candidates and parties.

the elections, with emphasis on technological readiness. Meanwhile the team has not addressed the other threats described above, nor has it involved civil society in the response, as other countries (such as Denmark) have done.[24]

In February 2019, the NCD sent all the political parties in Israel a special document intended to help them protect themselves against various cyber threats. The document specifies procedures and guidelines for strengthening their systems, websites, means of communication, and other virtual infrastructures, and addresses the protection of personal computers, the parties' internal networks, email, mobile phones, smart watches, and telephone exchanges. A particularly long section of the document is devoted to the protection of party websites, including details of what is required.[25]

Notwithstanding this activity, officials linked to the NCD clarified that this body is not obliged to deal with content relating to the elections system and does not intend to focus on frustrating campaigns intended to influence attitudes. However, in a debate in the Knesset in October 2018, just before the local authority elections, the NCD presented a cooperative initiative with Facebook to remove fake profiles.[26] Representatives of the Israeli Internet Association criticized this move, however, arguing that the NCD was not qualified to deal with this subject, even indirectly.[27]

When the date of the Israeli elections was published, Facebook announced that it was setting up a situation room in order to monitor information from a range of sources, including political parties and individual users, regarding posts and campaigns that breach its terms of use. The situation room was supposed to respond quickly to any violations of the rules. For this purpose, Facebook employed a censorship team, which used an artificial intelligence tool to highlight suspicious content. Another tool used by the team involved pushing back problematic campaigns, even if they were funded, in order to

---

24 "Summary of a Simulation Discussion on the Illegitimate Influence on Public and Political Debate by Digital Means, toward the 2019 Elections in Israel," Institute of National Security Studies, Israeli Institute of Democracy, and the Israeli Internet Association, February 26, 2019 [in Hebrew].

25 Ran Bar-Zik, "The Cyber Directorate Issues a Guide to Protection for Parties: Will They Learn the Lesson?" *Haaretz,* February 20, 2019 [in Hebrew].

26 Tal Shahaf, "The National Cyber Directorate: We Worked with Facebook and Twitter to Remove Thousands of Fake Accounts," *Globes*, October 15, 2018 [in Hebrew].

27 Omer Kabir, "Thousands of Fake News Accounts Exposed, which Tried to Influence the Municipal Elections in Israel," *Calcalist,* October 15, 2018 [in Hebrew].

diminish their appeal. Facebook also provided training for Knesset members and their parliamentary assistants who wanted to know how they could avoid misusing the platform, even giving advice on how to protect political accounts from hackers who could break in and issue false announcements from them.[28]

In mid-February 2019, Facebook announced it was increasing its efforts to avoid influencing the elections in Israel, including a "clean up" of followers of politicians. In this campaign, fake and bot accounts were removed from the network and also removed from the profiles of parties and candidates. Facebook even offered media personnel a tool for reporting networks of fake users.[29] Moreover, in mid-March 2019, the Facebook transparency tool for political announcements came into force in Israel, and thus Israel became the fifth country in the world to use this tool, which is intended to combat the threat of foreign interference and anonymous propaganda.[30]

At the beginning of January 2019, a number of lawyers submitted a petition to the Central Elections Committee, asking it to extend the laws of election propaganda to include propaganda on the internet. The petition included a request to the chairperson of the committee to issue an injunction forbidding the parties participating in the elections, or entities acting for them—whether or not for payment—from publishing any announcement, notice, response, "talkback," or "like" that did not carry the name of the party or the candidate on whose behalf it was published. In addition, the petition asked for an injunction forbidding the parties to pay any entity that did so on their behalf or in their name and to apply the injunction to all ads and posts on social media, SMS, and instant messaging programs.[31] The chairperson of the Central Election Committee accepted the petition and at the end of February 2019 set a precedent by issuing an order that required parties to identify themselves on any kind of propaganda on the internet and

28 Uri Berkowitz, Oshrit Gan El, and Tal Shahaf, "Bots, Fake News or Stories: What Will Determine the Fate of the Next Elections?" *Globes*, December 27, 2018.

29 Anat Bein-Leibowitz, "Facebook Embarks on a Campaign to Remove Fake Accounts In Israel; in its Sights – The Bots of Netanyahu and Gabbay," *Globes*, February 20, 2019 [in Hebrew].

30 Hagar Buchbut, "Just before the Elections: A Fast Form for Reporting Bots and the Facebook Transparency Tool," *Ynet,* March 14, 2019 [in Hebrew].

31 Yasmin Yablonka and Tal Shahaf, "An Ancient Law and Netanyahu's Objection: Is it Possible to Supervise Propaganda on the Internet?" *Globes*, January 8, 2019 [in Hebrew].

social media. On the grounds for this decision, the committee's chairperson stressed that, apart from the legal obligation, anonymous propaganda makes it difficult for the security forces to dispel suspicions of foreign intervention in the Knesset elections.[32]

At the end of February 2019, several internet and data security experts asked the Central Elections Committee to take steps prior to the Israeli elections to identify attempts to create fake online identities, particularly on social media. The experts expressed fears that foreign elements might try to interfere in the elections by using social media to spread fake information and manipulate users in other ways and called for the appointment of an official to coordinate reports of fake accounts designed to influence the election process. The model they wished to create is similar to the model that Israel has used against incitement on social media.

Currently, the state has no legal authority to force networks such as Facebook or Twitter to remove posts. There is, however, an interface enabling users to report and request the removal of posts that amount to incitement or breaches of the law: The Cyber Department of the office of the state attorney contacts the relevant network and asks for such material to be taken down. According to the state attorney's data, in about 85 percent of cases, the networks have responded positively to the request.[33]

Apart from the above, citizens held several initiatives to mark propaganda in a clear and consistent way, to avoid the use of fake accounts, and to indicate bots. In this framework, they pledged not to make use of any personal information in order to manipulate individuals emotionally and to secure campaign information, including by means of encrypting personal messages and securing databases.[34] A special online form was created enabling social media users to submit quick and effective reports about bots, suspicious accounts, and anonymous election propaganda, thus facilitating more effective handling of the problem on the various platforms.[35]

---

32 Daniel Dolev, "The End of Anonymous Propaganda: Parties Must Identify Themselves in Online Advertising," *Walla*, February 27, 2019 [in Hebrew].

33 Daniel Dolev, "Request to the Chairman of The Elections Committee: Act Against Online Attempts to Influence the Elections," *Walla*, February 25, 2019 [in Hebrew].

34 Guy Luria and Tehilla Shwartz-Altshuler, "Committing to Fair Elections Online," Israel Institute for Democracy, February 16, 2019 [in Hebrew].

35 Buchbut, "Just Before The Elections: A Fast Form for Reporting Bots and the Facebook Transparency Tool."

Most efforts to defend against foreign interference in the elections clearly were civilian initiatives, and we do not know about specific state preparations for such defense, notwithstanding the announcement by the GSS that "the security system is able to ensure the process of free, democratic elections."[36] The Central Election Committee also announced that "together with security personnel, the Committee has studied what happened in other countries and is formulating an outline of action."[37]As of the time of this writing, it is not clear if there were any foreign attempts to influence the elections to the twenty-first Knesset, or whether efforts to stop such attempts (if they existed) were successful.

It can be noted marginally that early in 2019, the state comptroller announced that he had instructed his staff to prepare for an audit of social media and for cyberspace and to examine the readiness of the authorities to protect themselves against cyberattacks on the computerized systems required for holding elections.[38]

Conclusion

The purpose of this article was to survey the steps taken to protect against the possibility of foreign interference in the Knesset elections in 2019, given similar attempts in other democratic countries in recent years. Until now, hardly any such attempts have been exposed to the Israeli public although the use of unidentified accounts or fictitious accounts in the framework of the internal political debate have been revealed.

The public's focus on the internal debate highlights the need to regulate the use of networks during election campaigns in particular and in terms of the democratic process in general. First, it is necessary to distinguish between various aspects of the phenomenon, and, above all, the use of bots, as political parties may operate or hire the services of companies who operate bots in order to promote their positions or to harm rival candidates. The use of bots should be deemed legitimate, providing it complies with the instructions of the head of the Central Elections Committee regarding

36 Amnon Abramowitz, "The GSS: 'We Have the Tools to Frustrate Foreign Attempts to Influence the Elections," *News 12,* January 8, 2019 [in Hebrew].

37 Dafna Liel, "Elections 2019: Preparing Action against Foreign Interference," *News 12,* January 9, 2019 [in Hebrew].

38 Buchbut and Adamker, "Head of the GSS Warns: A Foreign Country Is Planning to Interfere in the Elections in Israel."

the need to publish the name of the party or candidates in whose name the material is distributed.

Second, with respect to the publication of fake information, it is hard to envisage a fast and relevant mechanism (not a legal process) that would be able to determine which information is fake and which is genuine. The distance between such a mechanism and the risk of serious damage to freedom of expression is quite small. Therefore, it is suggested to allow the publishing of any information, even if some would define it as fake information, as a legitimate part of the democratic debate. Any person or organization who feel themselves injured by such publication can implement their right to seek redress from the legal system with a libel case or claim for damages.

Finally, regarding the use of unidentified profiles by individuals (not by parties), Twitter allows users to have anonymous accounts. Such an account is very important, as it permits people who are not able or willing to expose their identity (for example: state employees) to participate in the political debate and thus realize their right to express their views freely. The situation is quite different regarding the activity of foreign elements seeking to influence the democratic process; this kind of foreign activity amounts to blatant meddling in Israel's democratic process, which should be seen as illegitimate and must be opposed.

The best defense against foreign attempts to interfere in the 2019 Knesset elections clearly came from measures to protect against classic cyberattacks. As of yet, the Israeli public have not learned of any organized, methodical ability (if it even exists) to protect against attempts by foreign elements to exert influence. Defense against such attempts should include a number of basic components. First is intelligence, with the aim of collecting information from a range of sources, both overt and covert. Second, it is also vital to be able to research and analyze the data in order to build a picture of the situation and identify foreign and hostile efforts to influence the democratic process. This includes being able to distinguish between the domestic (legitimate) debate and the external debate, which should be prevented.

We can list a number of ways to thwart foreign attempts. First, the campaign should be exposed to the public, all while maintaining the confidentiality of sources, if necessary. Such exposure can remove the sting from a campaign and minimize its effect on the public. Second, it is possible to contact the media companies concerned, show them the information and demand its

removal, while also blocking the relevant user accounts. Finally, it is possible to proactively engage with the elements behind the campaign in order to thwart their plans.

Achieving this requires cooperation between organizations and technologies. The proposal is to set up a special task force to coordinate activity, based on the abilities of all the defense organizations in Israel. Due to the subject's sensitivity, the team should be directly subordinate to the Central Elections Committee or another apolitical entity. The special task force must acquire—and, if necessary, define and develop—technological tools to help it achieve its objectives.

Over the next two years, more than twenty election campaigns will take place in Europe and North America. We can assume that other countries will have strong interests in the outcomes of these elections, and there are even indications that attempts to interfere in them will occur.[39] Therefore, any lessons learned about the efficacy of steps to defeat foreign meddling in elections in Israel could have great importance for other countries expecting to hold elections.

39 Michael Chertoff and Anders Fogh Rasmussen, "The Unhackable Election: What it Takes to Defend Democracy," *Foreign Affairs* 98, no. 1 (2019): 157.

The INF Treaty and New START: Escalation Control, Strategic Fatalism, and the Role of Cyber

Stephen J. Cimbala

The fate of the Intermediate Nuclear Forces (INF) Treaty originally signed in 1987 between the United States and the Soviet Union now appears uncertain, since the United States has announced its intentions to withdraw from the agreement and Russia has stated it is prepared to respond accordingly. The significance of the withdrawal from the INF Treaty affects not only the immediate force sizes and structures but also the dynamics of nuclear deterrence in Europe and more broadly. Nowadays and in the future, the assessment of nuclear forces will be based on their agility, flexibility, and responsiveness to diverse circumstances of nuclear crisis management or of limited deterrence failure. As such, the significance of "cyber" grows accordingly: The "smartness" of deterrent forces, including their suitability for escalation control and for conflict termination, depends upon their information-dependent system integrity and resilience, especially if the template is complicated by the addition of missile defenses to the equation.

Keywords: Escalation control, nuclear war termination, cyberwar, INF (Intermediate Nuclear Forces) Treaty, arms control, nuclear modernization, deterrence, European security, missile defense, information warfare, crisis management

Stephen J. Cimbala is Distinguished Professor of Political Science at Penn State Brandywine.

Cyber, Intelligence, and Security | Volume 3 | No. 1 | May 2019

Introduction

Political leaders and expert commentators have already pronounced the Intermediate Nuclear Forces (INF) Treaty a dead letter.[1] The possibility of a slowdown or even retrenchment in US-Russian nuclear arms control cannot be excluded.[2] The decision to jettison the INF Treaty and the implications of that decision for the New START (Strategic Arms Reduction Treaty) are often discussed in terms of alleged American or Russian violations of technical protocols. This perspective is important but insufficient. In the following discussion, we first consider the assumption of a world without the INF Treaty and its implications for deterrence stability and escalation control in Europe. Second, we discuss the New START, which could be taken hostage by a US-Russian confrontation in a post-INF world. Third, we assess the significance of US missile defenses as potential wildcards in determining the probable degree of US-Russian strategic nuclear stability with, or without, New START and the INF Treaty in place. Crossing over all these topics is the increasing future significance of military cyber technologies and its implications for nuclear deterrence stability.

The INF Imbroglio

President Donald Trump and Secretary of State Mike Pompeo have announced that the United States will withdraw from the INF (Intermediate Nuclear Forces) treaty. Signed in 1987 between the United States and the Soviet Union, the agreement was a milestone in nuclear arms control, requiring both NATO and the Soviet Union to remove from Europe all land-based

1 The full name of the INF treaty is the Treaty between the United States of America and the Union of Soviet Socialist Republics on the Elimination of their Intermediate-Range and Shorter-Range Missiles. The treaty includes ground-launched ballistic or cruise missiles with ranges from 500 to 5,500 kilometers, whether nuclear or conventionally armed. The treaty was signed by US President Ronald Reagan and Soviet General Secretary Mikhail Gorbachev on December 8, 1987.

2 Expert assessments include William Tobey, Pavel S. Zolotarev, and Ulrich Kuhn, *The INF Quandary: Preventing a Nuclear Arms Race in Europe – Perspectives from the U.S., Russia and Germany*, *Russia Matters*, Issue Brief, January 2019, Belfer Center for Science and International Affairs, Harvard Kennedy School, https://www.belfercenter.org/publication/inf-quandary-preventing-nuclear-arms-race-europe-perspectives-us-russia-and-germany; and Steven Pifer, "Is There a Glimmer of Hope for the INF Treaty?," Brookings, December 27, 2018, https://www.brookings.edu/blog/order-from-chaos/2018/12/27/is-there-a-glimmer-of-hope-for-the-inf-treaty/.

ballistic and cruise missiles with estimated ranges between 500 and 5,500 kilometers. Trump's announcement of US plans to depart the INF agreement followed charges by the Trump and Obama administrations that Russia did not comply with the terms of the treaty due to its deployment of the SSC-8 ground-launched cruise missile (Russian 9M729). Russia has denied violations and has accused the United States of having deployed missile defense systems in Europe that could be repurposed as offensive strike systems within the treaty-prohibited ranges.[3]

Critics of Trump's decision to depart the INF Treaty expressed concern not only about the agreement per se but also about the implications of the US abrogation for the larger climate of US-Russian nuclear arms control. A deteriorating relationship between the United States and Russia over the INF Treaty could spill over into disagreement over extending the New START for strategic nuclear arms limitation, which was signed in 2010. Failure to extend the New START for five years in 2021 would leave the world's two nuclear superpowers without a reliable regime for limiting the numbers of nuclear warheads deployed on missiles of intercontinental range and on heavy bombers. In addition, the New START provides for inspections to verify the status of deployed warheads and launchers for each state, increasing

3 For background and perspective, see Lawrence J. Korb, "Why it Could (but Shouldn't) be the End of the Arms Control Era," *Bulletin of the Atomic Scientists*, October 23, 2018, https://thebulletin.org/2018/10/why-it-could-but-shouldnt-be-the-end-of-the-arms-control-era/.

See also Michael R. Gordon, "Russia Warns U.S. Moves Threaten 2011 Nuclear Pact," *Wall Street Journal*, January 15, 2019; Thomas Grove, "Putin Threatens Arms Race as U.S. Proposes to Exit Nuclear Treaty," *Wall Street Journal*, December 6, 2018; Pavel Podvig, "Russia Insists it is in Compliance with the INF Treaty," Russian Strategic Nuclear Forces, November 26, 2018, http://russianforces.org/blog/2018/11/russia_insists_it_is_in_compli.shtml; Rick Gladstone, "In Bipartisan Pleas, Experts Urge Trump to Save Nuclear Treaty With Russia," *New York Times*, November 8, 2018; Dmitry Stefanovich and Malcolm Chalmers, "Is This the End of Nuclear Arms Control?" *RUSI Newsbrief*, November 7, 2018, https://rusi.org/publication/newsbrief/end-nuclear-arms-control; Dmitri Trenin, "Back to Pershings: What the U.S. Withdrawal From the 1987 INF Treaty Means," Carnegie Moscow Center, October 24, 2018, https://carnegie.ru/commentary/77568; Steven Pifer, "The Trump Administration is Preparing a Major Mistake on the INF Treaty," Brookings, October 19, 2018; Ann M. Simmons, Thomas Grove, and Courtney McBride, "Russian Officials Slam Trump's Plans to Exit Nuclear Treaty," *Wall Street Journal*, October 22, 2018.

the transparency of each state's deployments, and therefore contributing to mutual trust.

Another by-product of discarding the New START and the INF Treaty could be an open-ended nuclear arms race in terms of deployments of strategic and non-strategic nuclear weapons (NSNW) in Europe and Asia.[4] Russia has been skeptical of INF restrictions for many years, as China and other states increased their deployments of intermediate and shorter-range ballistic missiles, while Russia's arsenal remained a treaty-compliant nullity. Officials in the Trump administration have also noted China's growing inventory of ballistic missiles as one reason for their decision to withdraw from the INF Treaty. According to experts, China views its land-based missiles armed with conventional warheads as "a pillar of their warfighting strategy" and useful across the spectrum of conflict.[5] As Jacob Stokes has noted,

> China plans to threaten or use its conventional missile arsenal against both regional countries and U.S. military assets and bases in Asia in the event of a future regional conflict, including one over Taiwan or islands in the East or South China seas. If such a conflict were to occur, experts assess China would use its conventional missiles to destroy its opponent's key military targets, starting with reconnaissance and early warning, command and control and air defenses, before moving on to missile sites, aircraft and ships.[6]

As a non-signatory to the INF Treaty, China has no legal obligation to limit its development and deployment of ballistic missiles over any ranges. US foreign and defense strategy, as well as nuclear posture statements, are focused on Russia and China as the principal threats to the United States and allied security—along with Iran and North Korea as important but lesser threats.[7]

---

4 Mikhail Gorbachev and George P. Shultz, "We Participated in INF Negotiations. Abandoning it Threatens Our Very Existence," *Washington Post*, December 5, 2018.

5 Jacob Stokes, "China's Missile Program and U.S. Withdrawal from the Intermediate-Range Nuclear Forces (INF) Treaty," U.S.-China Economic and Security Review Commission, February 4, 2019, https://www.uscc.gov/sites/default/files/Research/China%20and%20INF_0.pdf.

6 Ibid., p. 4.

7 Grateful acknowledgment is made to Dr. Jacob W. Kipp for insights pertinent to this section. See also Dmitri Trenin, "Russian views of US nuclear modernization," *Bulletin of the Atomic Scientists*, January 2019, https://thebulletin.org/2019/01/russian-views-of-us-nuclear-modernization/.

Possible side effects from removing the constraints of the INF Treaty include not only an arms race in regional nuclear and missile deployments but also an unintentional blowback that reduces effective decision time for warning, crisis management, and nuclear response. One reason for signing the treaty in 1987 was because of the short flight times to their intended targets that the Soviet SS-20 IRBMs (intermediate-range ballistic missiles) and NATO's "572" deployments were presumably capable of achieving. Key cities in western Russia or in NATO's Europe could be attacked with little warning compared to that provided by land or sea-based intercontinental missiles of longer range. Reintroducing medium and intermediate ground-launched missiles into Europe could exacerbate a crisis by encouraging nations to place their respective nuclear attack warning and command-response systems on hair-trigger alert and prepared for prompt launch. Something like this happened in November 1983 when the NATO command post exercise Able Archer was in danger of being misconstrued by some Soviet observers as an actual alliance decision for nuclear release.[8] As Jon B. Wolfsthal has noted,

> In particular, the fear that misunderstandings could drive leaders on either side to make rash nuclear decisions for fear that decision time was short led to the negotiation of the 1987 Intermediate-Range Nuclear Forces Treaty, an agreement now on the chopping block.[9]

Other implications of the apparent US decision to depart the INF Treaty are more explicitly political in nature. One issue is the impact of dissolving the agreement on the political cohesion of NATO. Many European members of NATO might prefer to have the treaty remain in place even if either or both sides nibbled at the edges of noncompliance. From the standpoint of many Europeans, NATO's credibility as a deterrent to Russian aggression against a member state is less a matter of comparing numbers of deployed forces than it is about the reliability of the US nuclear guarantee for its allies. A wider spectrum of nuclear options for NATO and for Russia, with respect to the yields of warheads and the diversity of launchers on each side, carries

8 Ben B. Fischer, "Intelligence and Disaster Avoidance: The Soviet War Scare and US-Soviet Relations," Ch. 5 in *Mysteries of the Cold War*, ed. Stephen J. Cimbala (London: Routledge, 2018), pp. 89–104.

9 Jon B. Wolfsthal, "With Russia and the US, Nuclear Risks Never Go Out of Vogue," Russia Matters, November 8, 2018, https://www.russiamatters.org/analysis/russia-and-us-nuclear-risks-never-go-out-vogue.

the risk of prioritizing the graduation of nuclear response to the certainty of it. From this perspective, Russia must not be permitted to believe that it can bite off an arm or leg of NATO territory and remain immune to high-end conventional or nuclear response directly on Russian territory.

The alternative perspective is offered in the Trump administration's Nuclear Posture Review of 2018. From this standpoint, the United States and NATO require a wider spectrum of nuclear options in order to have a credible deterrent against Russian provocations short of unlimited nuclear war.[10] Russia might believe that it could "escalate to de-escalate" a conventional war in Europe that was going badly for Russia by engaging in nuclear-first use as a bargaining chip to deter further NATO resistance or escalation. This view holds that a wider spectrum of nuclear options creates a more believable message with respect to intrawar deterrence and escalation control than a narrower range of choices.[11]

In some sense, we are back to the concept of limited war as a generator of risk, as Thomas Schelling has so expertly discussed it.[12] That is, what is most important about a limited nuclear war is not the damage that has already taken place but rather the relationship between that damage and the opponent's expectation about what further damage might ensue. This expectation will be based partly on the opponent's estimate of the first side's capabilities but also on its estimate of the first side's resolve in continuing up the ladder of escalation if its demands are not met. What is being tested

10 The case for nuclear flexibility is explained in Keith B. Payne, "Nuclear Deterrence in a New Era: Applying 'Tailored Deterrence,'" *National Institute for Public Policy* no. 431, May 21, 2018, http://www.nipp.org/2018/05/21/payne-keith-b-nuclear-deterrence-in-a-new-era-applying-tailored-deterrence/.

11 Stephen J. Cimbala, "The Trump Nuclear Posture Review: Three Issues, Nine Implications," *Strategic Studies Quarterly* 12, no. 2 (Summer 2018): 9–16. See also Payne, "Nuclear Deterrence In a New Era: Applying 'Tailored Deterrence'; and Nikolai N. Sokov, "Why Russia Calls a Limited Nuclear Strike 'De-escalation,'" *Bulletin of the Atomic Scientists*, March 13, 2014, https://thebulletin.org/2014/03/why-russia-calls-a-limited-nuclear-strike-de-escalation/.

12 Thomas C. Schelling, *Arms and Influence* (1966; New Haven: Yale University Press, 2008).

in this instance is the capacity of both sides for risk management under conditions of uncertainty.[13]

The Priority of Risk Management

The significance of the preceding observation goes beyond the specific scenarios of escalation and limited nuclear war in Europe. In the second nuclear age, following the end of the Cold War and the demise of the Soviet Union, the major challenges to nuclear-strategic stability may occur in regions outside of Europe: the Middle East, South Asia, and East Asia.[14] In those settings, states and their leaders will be tested not only on their ability to practice deterrence per se but will also be expected to rise to the demands of risk management under conditions of uncertainty. Insufficient thought has been given to this problem, even in scenarios of an outbreak of major war in Europe, and even more so, with regard to Middle Eastern and Asian contretemps. What, for example, do we reliably know about the perspectives held by the leaders in Iran, Pakistan, or North Korea on risk management with respect to nuclear escalation? Precious little is the answer, based on what is available in the public domain.

The challenge of risk management in and outside of Europe is also related to the arguments for or against retaining the INF Treaty and or New START. With respect to the INF agreement, a proliferation of medium- and intermediate-range missiles within Europe creates a Pandora's box of scenarios for which escalation management, including the problems of intrawar deterrence and war termination, have been thought through only superficially. War games at think tanks and war colleges may delve into these issues, but the analysis and discussions are confined largely to audiences of expert analysts, scholars, former diplomats, and military commanders. The diffusion of findings from these and other studies into the DNA of policy makers is a more complicated problem. Harvard's Kennedy School emphasizes the importance of the difference between "policy formulation" and "policy

13 Some experts doubt that any shooting war between the United States and Russia could be contained below the nuclear threshold. See Paul Goble, "Any US-Russia Military Clash 'Highly Likely' to Escalate into Nuclear War, Arbatov Says," *Eurasia Review*, December 5, 2018, https://www.eurasiareview.com/05122018-any-us-russia-military-clash-highly-likely-to-escalate-into-nuclear-war-arbatov-says-oped/.

14 Paul Bracken, *The Second Nuclear Age: Strategy, Danger, and the New World Politics* (New York: Henry Holt/Times Books, 2012).

implementation" for very good reasons. The implementation of policies requires a currency conversion: from good ideas and theoretical insights into procedures, routines, and standard operating procedures that organizations have rehearsed and practiced under realistic operational conditions.

Cold War experience with nuclear crisis management is a reminder of the difficulty in getting policy makers and operators on the same page with respect to signaling determination and conciliation at the same time. During the Cuban missile crisis, for example, President Kennedy and members of the ExComm (his senior advisory group for crisis management) sought to convey to Soviet Premier Khrushchev that the United States was determined to have Soviet medium- and intermediate-range missiles removed from Cuba. But the United States also sought to achieve this objective without military escalation that could lead to an outbreak of war with the Soviet Union, including possibly expanding that war into a nuclear conflict. Accordingly, the United States instituted a blockade or quarantine against Soviet ships headed to Cuba. This decision was intended as a limited escalation in order to give the Soviets an option for a face-saving retreat without horizontal or vertical escalation.

Throughout the tense thirteen days of the Cuban missile crisis, leaders were plagued by misperceptions of intentions and "normal" bureaucratic behavior that created dysfunctional speed bumps in the way of conflict resolution. In the American case, a U-2 reconnaissance plane on a routine mission wandered into Soviet air space, causing Soviet fighters to scramble; a scheduled test launch of a US intercontinental ballistic missile (ICBM) from California went ahead despite the heightened alert levels on both sides; and, an American U-2 was shot down over Cuba based on the decision made by a local Soviet commander. On the Soviet side, in addition to the deployment of medium-range ballistic missiles (MRBMs) and (IRBMs), the Soviets also deployed nuclear-capable tactical missiles with their ground forces in Cuba, with the understanding that ground force commanders could use those missiles in the event of an American invasion of Cuba. As the crisis reached its denouement, Cuban leader Fidel Castro urged Khrushchev that the Soviet Union should launch a preemptive nuclear-first strike against the United States. Castro claimed to have incontrovertible evidence that the United States was preparing for an imminent attack on Cuba. As Khrushchev recalled,

> Only then did I realize that our friend Castro, whom I respect for his honesty and directness, had failed to understand us correctly. We had installed the missiles not for the purpose of attacking the United States, but to keep the United States from attacking Cuba. What does it mean to make a preemptive strike? We could deliver the first blow, but there would be an immediate counterblow—both against Cuba and against our own country.[15]

Of course, Khrushchev had additional motives for deploying nuclear missiles in Cuba, including an attempt to change the perceived balance of strategic nuclear-missile power between the United States and the Soviet Union. However, he was able to climb down the ladder of escalation because the US management of the crisis offered an option between provocation and conciliation. The United States publicly accepted removal of the Soviet nuclear-capable missiles from Cuba in return for an American promise not to invade Cuba. In addition, the United States also secretly agreed to the eventual removal of Jupiter medium-range missiles from Turkey, about which the Soviets had previously complained.

These reflections on the Cuban missile crisis are not a distraction from our present endeavor, but a warning. As dangerous as the crisis was for humanity, it benefited from a simple structure of social action. Two governments shared responsibility for starting the crisis and for ending it. In the United States and the Soviet Union, political leadership exercised authoritative control over the armed forces. Although the allies' needs and expectations figured into Soviet and American decision making, the crisis was about the strategic nuclear relationship between two superpowers and the stealthy attempt by Khrushchev to adjust the perception of that balance.

In contrast, now consider a future crisis in Europe between NATO and Russia. NATO has expanded to twenty-nine countries from sixteen during the Cold War. In theory, a decision to invoke Article 5 in favor of collective military action requires unanimous consent of member states, as represented in the NATO Council. In this large and heterogenous group, it will be sufficiently difficult to reach a consensus in favor of any military action unless the Russians plump for an all-out invasion of Western Europe with the objective of dismantling NATO and occupying its remains. However,

15 Jerrold L. Schecter *Khrushchev Remembers: The Glasnost Tapes*, trans. and ed. Vyacheslav V. Luchkov (Boston: Little, Brown, 1990), p. 177.

Russia lacks the military capability to impose such a coup de main on NATO. Therefore, it is more likely that Russia will seek to use its capacity for hybrid warfare, combining unconventional and conventional military steps, in order to politically divide NATO. An infiltration of Estonia or Latvia by "little green men," combined with selective air and ground attacks in the Baltics and an extensive propaganda and disinformation campaign, could create a united NATO response; but such a campaign could also divide NATO into resisters and ambivalents, depending on who was threatened and to what extent.

Suppose, in the preceding case, NATO reacts with collective unity and begins to turn the military tide against Russia, with NATO's capabilities for conventional deep strike used against Russian forces engaged in fighting on NATO members' territory. Russian reinforcements from its western military districts come to the rescue of their besieged comrades in the Baltics, and NATO responds with air- and sea-launched strikes against Russian forces as they cross the border from Russia into Latvia. Russia interprets this last NATO move as an attack on its homeland and, in response, fires a warning shot in the form of an electromagnetic pulse burst that shorts out electronics throughout much of the battlespace and surrounding territories. The United States places its strategic nuclear and theater nuclear forces on higher levels of alert while continuing its conventional deep strikes into Russian-occupied Latvia or Estonia and across the border into Russia. Russia also alerts its strategic and theater nuclear forces and both states' nuclear C3 (command, control, and communications) systems are now on the *qui vive*.

This situation would be complicated enough with the present deployments of theater nuclear and conventional weapons in Europe. Adding in unlimited numbers of ground-launched medium- and intermediate-range missiles, per the demise of the INF Treaty, only complicates the challenge of nuclear risk management in this or any related scenario. Granted, the United States and Russia also have sea- and air-launched weapons that could contribute to intra-theater deterrence (or escalation, depending on the case). However, ground-launched missiles have the special character that their prompt strike capabilities and locations invite preemptive attack on themselves. Their launchers are at known, easily detectable locations and could be destroyed with conventional as well as nuclear weapons. Once nuclear forces have been alerted and the possibility of escalation across the nuclear threshold cannot be excluded, military leaders will be pressing for the early destruction of

MRBMs and IRBMs that are nuclear capable. Knowing this, Russian leaders may fear a situation in which they must "use them or lose them" and within a very small time for decision (shorter than the time assumed available for decision and response to a strategic nuclear attack by the United States on Russia or vice versa).

With respect to this or other possible scenarios in the European theater of operations, the United States and Russia might consider maintaining the INF Treaty in some revised form. Instead of banning all missiles of a certain range, they might agree to permit conventionally armed, but not nuclear-capable, ground-based delivery systems. An inspections regime could be established to verify that MRBMs and IRBMs deployed in Europe by either side are equipped only with conventional warheads. Russia would be free to deploy MRBMs and IRBMs (to an extent) and NATO could respond with symmetrical (more or less) deployments of its own. Verification of non-nuclear status would be more challenging for air-launched or sea-based systems, but not impossible. In any case, air-launched and sea-based weapons are less in need of verification, compared to ground-based systems, because they are less provocative from the standpoint of crisis stability. The known locations of ground-based systems make them potentially attractive targets for preemption.

One reason that the United States is better off with—as opposed to without—the INF agreement is that Russia has the advantage of being able to deploy intermediate and shorter-range ground-based missiles on its own state territory. On the other hand, if the United States sought to deploy ground-based missiles in Europe within range of Russia (or, for that matter, in Asia within range of China), consent of a willing ally to host those missiles and launchers would be needed. If those missiles were nuclear capable, the burden of acceptance on the part of US, European, or Asian allies would be even greater. This is part of the reason why European government officials have attempted to act as intermediaries between the United States and Russia in order to preserve the present INF Treaty. In addition, European leaders have urged the United States to build a more persuasive case for departing from the INF Treaty so that blame in the "public square" falls on Russia and not on the United States or NATO. As noted by one unidentified European diplomat, "The US administration needs to take the Europeans with them.

It's important that if the agreement fails it is clear to everyone that it is the Russians' fault. I think the administration gets this."[16]

Perhaps with the preceding points in mind, Russia steadfastly has blamed the United States for the probable demise of the INF Treaty, has denied any accusation of cheating, and has pointed to alleged US infractions of the agreement. Russian Deputy Foreign Minister Sergei Ryabkov reaffirmed Russia's refusal to accept responsibility for a failed treaty in November 2018:

> We believe that the US plans to withdraw from the INF Treaty, in case (this scenario) is implemented, will trigger a grave aftermath for European and global security. We deny any logic that tries to attribute to us actions, which allegedly pushed Washington to declare the plans to withdraw from the treaty.[17]

US decisions to withdraw from the INF Treaty, first announced by President Trump in October 2018 and reiterated by Secretary of State Mike Pompeo in early February 2019, have pointed to Russia's refusal to bring its development, testing, and deployment of the 9M729 missile into compliance with the requirements of the treaty. Instead of seeking to enforce the agreement by further negotiation and bargaining with Russia, the United States has closed the door on finding a mutually satisfactory solution and has offered to Vladimir Putin a putative excuse for Russian INF-range missile modernization and deployment, including in Europe.[18] In addition, the apparent demise of the INF Treaty, amid a poisoned political atmosphere between Washington and Moscow, has increased the likelihood of a total collapse of the US-Russian nuclear arms-control regime, including the future of the New START.

---

16 Julian Borger, "European Diplomats Mount Last-ditch Effort to Stop US Scrapping INF Treaty," *Guardian*, November 18, 2018.

17 "Diplomat Repudiates Narrative that Russia's Moves Drive US into Abandoning INF Deal," *TASS*, November 19, 2018, http://tass.com/politics/1031456.

18 US Aegis-ashore systems deployed in Eastern Europe could, from the Russian perspective, constitute a preparatory violation of the INF Treaty, given the potential capability of their launchers to fire conventional or nuclear armed Tomahawk cruise missiles against Russia. The United States retired its nuclear armed Tomahawk cruise missiles between 2010–2013 but could quickly reinstate the nuclear option for Tomahawk if deemed necessary. See Theodore Postol, "Russia May Have Violated the INF Treaty. Here's How the United States Appears to Have Done the Same," *Bulletin of the Atomic Scientists*, February 7, 2019, https://thebulletin.org/2019/02/russia-may-have-violated-the-inf-treaty-heres-how-the-united-states-appears-to-have-done-the-same/.

The possible end to the INF Treaty is also connected to the durability of the entire Russian-American nuclear arms-control regime, including the fate of the existing New START on strategic nuclear arms limitation. New START will expire in 2021 unless automatically extended by both sides for another five years. The agreement limits each state to a maximum number of 1,550 warheads on land-based intercontinental ballistic missiles (ICBMs), submarine- launched ballistic missiles (SLBMs), and heavy bombers. The New START also limits the numbers of operationally deployed and reserve delivery systems available to each state. Although some arms-control experts might regard the automatic extension of the New START until 2026 as a "no brainer," the present and foreseeable political climate as between the United States and Russia does not guarantee such an outcome. One Russian author has warned,

> There is one more detail of fundamental importance. If the two leading military powers have failed to curb the race in strategic nuclear forces, there is no chance that hypersonic weapons, space-based systems, long-range conventional missiles, and cybersecurity warfare activities will ever be controlled. The arms race will spread to other domains.[19]

The Challenge of Cyber

Cyberspace activity is an example of the "domain spread" that may contribute to a weakening of deterrence and crisis stability. Cyberwar has the potential to undermine some of the basic premises upon which nuclear deterrence and crisis stability are based, in a number of ways.[20] First, nuclear crisis management assumes a certain degree of transparency about actors' intentions and capabilities. Cyberattacks could interfere with the clarity of communication between crisis-bound adversaries and lead them to doubt otherwise reassuring

19 Andrei Akulov, "Responding to US Unleashing Unfettered Arms Race: Russia's Options," *Strategic Culture,* October 22, 2018, https://www.strategic-culture.org/news/2018/10/22/responding-us-unleashing-unfettered-arms-race-russia-options.html.

20 Andrew Futter, "Cyber Threats and Nuclear Weapons: New Questions for Command and Control, Security and Strategy," Royal United Services Institute for Defence and Security Studies (RUSI), *Occasional Papers* (July 2016), https://rusi.org/publication/occasional-papers/cyber-threats-and-nuclear-weapons-new-questions-command-and-control.

indicators of no enemy plan for preemptive or preventive strikes. Second, cyberattacks could be designed to directly compromise the performance of another state's warning, C3 (command, control, communications), intelligence, surveillance and reconnaissance systems, increasing fears of surprise attack, and willingness to launch on warning with less than unimpeachable information. As David E. Sanger has noted,

> The implications of having our own command-and-control system compromised underscore why sabotaging similar systems in other nations is dangerous business. If American leaders—or Russian leaders—feared their missiles might not lift off when someone hit the button, or that they were programmed to go off-course, it could easily undermine the system of deterrence that has helped reduced the likelihood of nuclear war for the past several decades.[21]

Third, states actively engaged in peacetime computer network exploitation, including the mapping of enemy systems and procedures as well as the insertion of malware that may be activated "on the day," will find it difficult to resist the temptation to accelerate this exploitation as the onset of a crisis seems imminent. The result might be that as a crisis moves from its early to its later stages, the information needed to resolve it is ever more transient and unreliable. Fourth, cybersecurity issues have, in the case of Russia and the United States, contributed to a toxic political atmosphere of mutual suspicion and doubt with respect to any larger and mutually agreeable enterprises. Alleged Russian interference in the US presidential elections of 2016, including the Russian Internet Research Agency (IRA) and military intelligence's (GRU) manipulation of social media in order to plant false narratives about American politics and culture, has tied the hands of US leaders who might otherwise want détente and a more positive relationship with Russia.

Fifth, in addition to the corruption of information via attacks on computers and networks, cyberattacks have reportedly been used to disable nuclear infrastructure, including centrifuges and nuclear launch systems.[22] Sixth, in the future, smarter information systems and artificial intelligence decision aids may appeal to policy makers or commanders as substitutes for the human

21 David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (New York: Crown, 2018), p. 299.

22 Ibid., pp. 41–47 and 268–279.

factor in ensuring against nuclear vulnerability. For example, Russia's Cold War-era "dead hand" system for postattack launch of remaining ICBMs even after the national command authority had been paralyzed by nuclear strikes could inspire a twenty-first century equivalent that delegated the final decision to a truly automated "doomsday machine" even more relentless than its predecessor. Seventh, cyber issues are central to the evolving relationship between antimissile defenses and the offensive missile attacks that they are intended to defeat. Cold War-era missile defenses were mainly a competition in physics and engineering. Although physics and engineering obviously still matter, the effectiveness of future US, Russian or other national missile defenses will be more and more dependent upon whether they are "state of the art" in information systems that support C4ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance).[23] In the case of national missile defenses, information systems must be able to provide accurate and timely warning and attack characterization; distinguish real threats from decoys; prioritize intercepts relative to the proximate threat posed by various attackers; and close the loop from sensor to decision maker to shooter faster than the opposing force is able to do.

Eighth, related to this greater dependency upon cyber performance for missile defenses is the increased significance of space-based platforms and their growing requirements for improved cybersecurity.[24] Already the United States and other spacefaring powers use space systems for reconnaissance, geolocation, communications, command-control, intelligence gathering, missile attack warning, and other vital functions in support of national defense and security.[25] The weaponization of space systems until now has been deflected by the Outer Space Treaty and by shared understandings that

23 Rebecca Slayton, *Arguments that Count: Physics, Computing, and Missile Defense, 1949–2012* (Cambridge: MIT Press, 2013), pp. 199–209 and passim.

24 The US Defense Intelligence Agency (DIA) notes that "China and Russia, in particular, are developing a variety of means to exploit perceived U.S. reliance on space-based systems and challenge the U.S. position in space." See Defense Intelligence Agency, "Challenges to Security in Space," January 2019, p. 7, https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf.

25 Adm. Dennis C. Blair (ret.), "Why the US Must Accelerate All Elements of Space-Based Nuclear Deterrence," Defense News, February 7, 2019, https://www.defensenews.com/opinion/commentary/2019/02/07/why-the-us-must-accelerate-all-elements-of-space-based-nuclear-deterrence/.

space is a "commons" that is available and necessary to all. However, future technology could enable the basing of missile defenses or other weapons in space with space-to-earth or space to space strike capabilities. The latter is imminent, depending on the orbital paths of existing and future satellites. For example, the United States, Russia, and China are reportedly working on "repair" satellites that could closely approach another "friendly" satellite in order to repair its malfunctions and to refuel it for additional missions. On the other hand, the technology that permits "repair" satellites to work enables the same orbiters to disrupt or destroy another "unfriendly" satellite, should they choose to do so. To deal with this situation of a possible form of mutual space vulnerability, states will have to negotiate "keep away" circumferential zones surrounding their satellites and may also need to equip those satellites with self-defense mechanisms.

Ninth, cyberwar might contribute to a mistaken decision for a nuclear-first strike or prompt retaliatory launch, on the faulty assumption that the opponent had already decided to attack, or that an attack was actually in progress. Cyberattacks have several properties that contribute to first strike fears. Firstly, they are hard to detect. Malware may be inserted into another state's networks months or even years in advance, primed for later activation or nearly instantaneous cyberattacks against enemy command-control and communications systems may precede a kinetic attack. Secondly, cyberattacks are often difficult to attribute. Attackers purposely disguise their identities and some may impersonate third parties, implicating an innocent state actor or others. Thirdly, attacks on critical infrastructure or information systems can create panic among targeted decision makers who might therefore decide to strike at the plausible sources of the attack before their own systems fail.

To mitigate this danger of contamination of nuclear deterrence stability by the possibility of mutual cyber destruction, states might attempt to establish certain "rules of the road" with respect to peacetime and crisis-time behavior in cyberspace. One option is increased transparency with respect to the capabilities of states' systems for offensive and defensive computer network operations. Just as nuclear arms-control agreements limit the numbers of launchers and warheads available to each side and provide for monitoring and verifying of agreed limits, the broad compass of cyber defense and attack capabilities could be made known without compromising actual code or in-house protocols. This suggestion collides with the traditional expectations

of secrecy that mark all states' cyber activities. On the other hand, in a cyber competitive world, secrets are sometimes perishable; yesterday's secret system is often tomorrow's exposure. Edward Snowden and the Shadow Brokers compromised some of the National Security Agency's most powerful tools for offensive cyber operations, the so-called Tailored Access Operations (TAO) instruction manuals and codes.[26] And the Stuxnet worm used successfully against Iran's centrifuges became a cause célèbre when it unexpectedly mutated into a global problem.[27]

Another option for the United States and other major nuclear and cyber powers would be to adopt an agreement on "no first use" of cyber as well as nuclear weapons during a crisis. Such an agreement would be a declaratory policy that relies upon the good faith of the participants: A cyber "first use" would be difficult to verify, compared to the obviousness of a nuclear-first use. The reasoning behind this agreement would be that successful crisis management requires contending parties to fully understand the other side's actual intentions and capabilities, regardless of their disagreements about other matters. An agreement of this sort might be supported by an exchange of cyber experts among countries in peacetime and by encouraging regular channels of communication between the US Cyber Command and their counterparts in other countries.

INF, New START, and the Control of Escalation

The previous discussion is meant to establish the priority of cyber-related deterrence and risk management in creating a future viable framework for nuclear deterrence and crisis stability. The examples of cyber relationships with nuclear deterrence and crisis stability are only part of the potential for a collision course between nuclear arms races and new technologies. Meanwhile and apart from new technologies, the nature of the linkage between the INF Treaty and New START in the minds of American and Russian planners remains an open question. If additional INF deployments are undertaken by either side, these deployments will have a two-sided possibility with respect to the ladder of nuclear escalation. First, they can serve as firebreaks between the initial or early use of tactical nuclear weapons, on one hand,

26 David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (New York: Crown Publishers, 2018), pp. 226–230.

27 Ibid., pp. 21–25.

and the employment of strategic nuclear forces, on the other. Second, and in contrast, new INF could serve as conveyers for a slippery slope of escalation that was undertaken in the mistaken expectation that theater nuclear war could be sealed off from strategic nuclear attacks. This two-sided character of the relationship between INF and strategic nuclear forces has an inherent ambiguity that might appeal to some deterrence theorists but, at the same time, alarms policy makers and military strategists looking for "exit ramps" in the event of an outbreak of tactical nuclear warfare.

The political linkage between the INF Treaty and New START is also subject to diverse interpretations. One school of thought holds that the demise of the INF Treaty may create a domino effect that has a high probability of toppling New START and creating other negative by-products for nuclear stability. Russian president Vladimir Putin noted in late November 2018 that Russia would not allow an American withdrawal from the INF Treaty to go unanswered. According to Putin, Russia's military and political leaders will be tasked to develop responses to US abrogation of the treaty. The Russian president cited his previous warnings to the United States against its withdrawal from the ABM (Anti-Ballistic Missile) Treaty limiting missile defenses and Russia's response, in the form of hypersonic weapons capable of defeating any defense. At the same time, however, according to Putin, Russia will not be dragged into a new nuclear arms race; instead, Russia will emphasize "balanced development" of its armed forces.[28] Other Russian officials, however, have warned that a US departure from the INF Treaty could collapse the entire nuclear nonproliferation system and increase the risk of nuclear war.[29]

Nevertheless, the INF Treaty and New START are not two peas in a pod. The INF Treaty is a long-standing agreement that dates from 1987 (going into effect in 1988) and signed on the eve of the Cold War endgame. It was a historic achievement for its time, creating a security space for nuclear threat reduction in Europe, and contributing to the rapprochement between US president Ronald Reagan and Soviet leader Mikhail Gorbachev, which helped to peacefully end the Cold War. Although a case can be made for

28 "Russia Won't Be Dragged into New Arms Race, but Will Respond to US Withdrawal from INF – Putin," *RT*, November 20, 2018, https://www.rt.com/news/444394-putin-russia-inf-arms-race/.

29 Ibid. See also "Kremlin Concerned Over US Attempts to Reject New START Treaty Extension," *TASS*, November 29, 2018, http://tass.com/politics/1033396.

continuing the agreement on grounds of arms control, the political winds between the United States and Russia have shifted considerably since the halcyon days of the early post-Cold War years and the bromance between US president Bill Clinton and Russian president Boris Yeltsin. Putin wants a multipolar world that includes a militarily resurgent Russia, fearful of NATO expansion, of US-supported "color revolutions" in states bordering on Russia or in Russia itself, and of US missile defenses that could pose a threat to Russia's nuclear deterrent.

In this context, extending the New START to 2026 or thereafter neither poses an existential threat to Russia nor requires it to invest scarce defense resources that threaten its fiscal solvency. The US nuclear modernization plan for the next several decades anticipates replacement of each of the three "legs" of its strategic nuclear triad of ICBMs, SLBMs, and heavy bombers.[30] However, this plan can be accomplished within the constraints of the ceilings on warhead and launcher deployments in New START.[31] US planners anticipate that each leg of the triad will undergo qualitative improvement but not necessarily an increase in the numbers of missile or warhead deployments.

Missile Defenses: Meaningful or Malign?

The matter of American and NATO missile defenses remains a point of contention between Washington and Moscow, with potential side effects for the viability of New START. Russia attempted unsuccessfully to get restrictions on US missile defenses included in the New START of 2010 and are likely to raise this point again, in connection with any agreement to extend New START. In addition, Russia may also bring into the conversation the issues of long-range conventional strike systems and military uses of

30 Jon B. Wolfsthal, Jeffrey Lewis and Marc Quint, *The Trillion Dollar Nuclear Triad: US Strategic Nuclear Modernization Over the Next Thirty Years* (Monterey: James Martin Center for Nonproliferation Studies, January 2014), http://cns.miis.edu/opapers/pdfs/140107_trillion_dollar_nuclear_triad.pdf.

31 US Congressional Budget Office, *Approaches for Managing the Costs of U.S. Nuclear Forces, 2017 to 2046* (Washington, DC: Congressional Budget Office, October 2017), www.cbo.gov/publications/53211.

space. Either the United States or Russia might also want to introduce the issue of cyberwar and its possible relationship to nuclear-strategic stability.[32]

Russia's proclivity for stuffing other issues into the New START negotiations, other than the limitations on offensive warheads and launch systems, complicates what might otherwise be a straightforward process. Russia's contention that US missile defenses deployed in Europe could be repurposed as offensive strike systems—part of their quibbling with respect to INF as well as New START—is stronger on military-technical grounds, as opposed to realistic political ones. The US Navy has established a program to develop hypersonic boost-glide weapons for multi-service use, including possible deployments on Ohio-class ballistic missile submarines converted to launch cruise missiles or Virginia-class attack submarines with a specialized payload module. Conceivably the hypersonic glide body could also be deployed on cruisers and destroyers, creating a large number of sea-based prompt global strike (PGS) weapons with a range reaching large areas of Russia and China. Although sea-based weapons are not included within the scope of the INF Treaty, weapons that could be launched from the Mk-41 Vertical Launch System (VLS) deployed on ships and submarines could also be launched from the same system deployed on land, including the Aegis Ashore based in Romania (and an additional system planned for Poland).[33] With regard to New START, hypersonic glide weapons deployed on Virginia-class submarines would not fall within its jurisdiction, but warheads deployed on Ohio-class ballistic missile submarine launchers for hypersonic boost-glide vehicles could be counted against allowable New START totals. According to experts from the RAND Corporation, Russian leaders emphasize the US development of advanced conventional capabilities—especially hypersonic glide vehicles and missile defenses—not

32 On this issue, see Futter, "Cyber Threats and Nuclear Weapons" and Stephen J. Cimbala, *Getting Nuclear Weapons Right: Managing Danger and Avoiding Disaster* (Boulder: Lynne Rienner, 2018), pp. 191–205.

33 Andrei Akulov, "More Details on Reasons Behind US Decision to Leave INF Treaty," Strategic Culture Foundation, November 25, 2018, https://www.strategic-culture.org/news/2018/11/25/more-details-on-reasons-behind-us-decision-to-leave-inf-treaty.html. See also Strategic Systems Programs, Department of the Navy, "FY19 – FY23 Navy Intermediate Range Conventional Prompt Strike (IRCPS) Weapon System (WS) Development and Integration Presolicitation Notice," Solicitation Number N00030-19-R-0025, November 21, 2018.

necessarily because of immediate jeopardy to Russia's strategic deterrent, but because these US systems, "especially if fielded in larger numbers, may become a greater threat to Russia's second-strike capability."[34]

With regard to the preceding military-technical factors, much depends on the specific direction of US research and development efforts as they move toward actual deployment. But it seems clear even now that the United States could realize any conventional PGS modernization objectives with sea-based and air-launched platforms, excluding land-based deployments based on repurposed missile defenses. Politics weighs in favor of NATO restraint with respect to ground-based PGS systems of intermediate or larger range. Given the hard work in getting NATO consensus on the European Phased Adaptive Approach (EPAA) to missile defenses, a turncoat operation converting defenses into offensive weapons would be neither politically expedient for NATO nor militarily efficient.[35] A repurposing of Aegis Ashore for offensive missions would alarm Russia without providing a meaningful gain in NATO's already extensive conventional and nuclear strike power. Without EPAA, what deters Iran or another regional actor from moving faster toward actual nuclear weaponization and deployment? Only deterrence and the threat of punitive retaliation do in the case of any hostile nuclear launch; without defenses, there can be no additional threat of deterrence by denial.

Russians know all this, but they prefer to use American and NATO missile defenses as a bargaining chip and a bugaboo because this ploy supports Putin's rhetoric of being surrounded by an advancing West, pulsing with prepackaged color revolutions exportable into Russia's security space. Putin's points of argument about US and NATO antimissile defenses are, at least at the margin, logically inconsistent. On one hand, the Russian president brags of Russia's new hypersonic weapons that will surely defeat any US or allied Western missile defenses. On the other hand, US and NATO missile defenses present a security threat to Russia sufficient enough to cause Russia's strategic and military-technical hyperventilation.

Russian fears on this point are of two kinds. First, missile defenses themselves, if sufficiently competent and strategically located on a regional

34 Christopher S. Chivvis, Andrew Radin, Dara Massicot, and Clint Reach, "Strengthening Strategic Stability with Russia" *Perspectives* (RAND Corporation) (2017), https://www.rand.org/pubs/perspectives/PE234.html.

35 For important background and perspective, see Andrew Futter, *Ballistic Missile Defence and US National Security Policy* (New York: Routledge, 2013), Ch. 5–7.

and global basis, could nullify Russia's nuclear deterrent by threatening its strategic nuclear second-strike capability. A second concern is that, even if present and immediately foreseeable defense technologies cannot by themselves threaten Russia's nuclear deterrent, defenses might be part of a larger military-strategic schematic for disarming Russia. From this standpoint, advanced US and NATO missile defenses combined with long-range, conventional strike systems, cyberwar, and space-based or space-enhanced weapons, together with NATO's own version of hybrid warfare, could confer a coercive advantage in crisis management.[36] This more elaborate scenario for putative Russian vulnerability probably has more to do with Russia's history of resistance to foreign invasions and the cultural DNA left by that experience than it does with military-technical or nuclear-strategic realities.[37]

For example, the idea that the United States might decide to launch a disarming conventional first strike against Russia's strategic nuclear forces—in the expectation that Russia would somehow accept defeat or retaliate only with its own conventional weapons—strains credulity. From a military-technical standpoint, there is no feasible way for the United States or NATO to accomplish Russia's effective nuclear disarmament with conventional strikes only. Russia's launch detection of a massive US attack on its state territory from land- and or sea-based missiles would be followed almost immediately by an order for "launch on warning" of its available nuclear forces. Russia would not wait to determine whether the fast flying US missiles were equipped with conventional or nuclear-armed warheads, nor, for that matter, would the United States. In theory, either side might wait until weapons had actually been detonated on its state territory before responding with nuclear counterattacks; but in practice, that choice is highly unlikely as heads of state will be urged by their military advisors that they face a "use them or lose them" dilemma with respect to silo-based intercontinental ballistic missiles (ICBMs).

---

36 Potential threats, mitigation options, and other aspects of US space operations receive expert consideration in Allison Astorion-Courtois, Robert Elder, and Belinda Bragg, "Contested Space Operations, Space Defense, Deterrence, and Warfighting: Summary Findings and Integration Report" NSI, 2018, https://nsiteam.com/social/wp-content/uploads/2018/11/Space-SMA-Integration-Report-Space-FINAL.pdf.

37 Richard Lourie, *Putin: His Downfall and Russia's Coming Crash* (New York: St. Martin's Press, 2017), pp. 130–142 and passim.

The competence of US and Russian strategic nuclear forces with respect to deterrence and crisis stability can be estimated and summarized in the following tables. Table 1 illustrates plausible New START-compliant force structures for the United States and for Russia within the constraints of a 1,550 limit on the numbers of operationally deployed warheads on strategic launchers for each side. Table 2 summarizes the outcomes of nuclear force exchanges for four different scenarios of operational readiness and launch doctrine: (a) forces are on generated alert and launched on warning, (b) forces are on generated alert and riding out the attack, (c)forces are on day-to-day alert and launched on warning and, (d) forces are on day-to-day alert and riding out the attack. Tables 3 and 4 repeat this process for US and Russian forces limited to a maximum of 1,000 peacetime deployed warheads.

Table 1: US-Russia Total Strategic Weapons, 1,550 Deployment Limit

United States	**2017 Plan**	**Dyad Without ICBMs**	**Dyad Without Bombers**	**Triad 10 SSBN 300 ICBM**
ICBM	400	0	400	561
SLBM	1040	1407	1148	880
AIR	109	109	0	109

Russia	**Balanced Triad**	**No Bombers**	**No SLBMs**	**ICBMs Only**
ICBM	758	907	1412	1502
SLBM	704	640	0	0
AIR	70	0	88	0

Source: Force structures are based on author's estimates and New START counting rules. See also US Congressional Budget Office, *Approaches for Managing the Costs of U.S. Nuclear Forces, 2017–2046* (Washington, DC: Congressional Budget Office, October 2017), and Pavel Podvig, *Russian Strategic Nuclear Forces* (blog), http://russianforces.org/. Grateful acknowledgment is made to Dr. James Scouras for use of his Arriving Weapons Sensitivity Model (AWSM@) for making the calculations and drawing the graphs. He is not responsible for any analysis or arguments herein.

Table 2: US-Russia, Surviving and Retaliating Warheads, 1,550 Deployment Limit

United States	2017 Plan	Dyad Without ICBMs	Dyad Without Bombers	Triad 10 SSBN 300 ICBM
GEN, LOW	1282	1219	1290	1297
GEN, ROA	887	1148	966	771
DAY, LOW	948	788	983	1006
DAY, ROA	603	766	659	530

Russia	Balanced Triad	No Bombers	No SLBMs	ICBMs Only
GEN, LOW	1303	1335	1335	1352
GEN, ROA	885	816	500	501
DAY, LOW	1080	1164	1290	1352
DAY, ROA	693	645	495	501

Source: Author, based on Arriving Weapons Sensitivity Model (AWSM@) designed by Dr. James Scouras, who is not responsible for any analysis here.

Table 3: US-Russia, Total Strategic Weapons, 1,000 Deployment Limit

United States	1000 Triad CBO	Dyad Without Bombers	Dyad Without ICBMs	SLBMs Only
ICBM	218	280	0	0
SLBM	672	720	890	960
AIR	109	0	109	0

Russia	Balanced Triad	No Bombers	No SLBMs	ICBMs Only
ICBM	318	288	858	1000
SLBM	608	704	0	0
AIR	74	0	76	0

Source: As in Table 1 above.

Table 4: US-Russia, Surviving and Retaliating Warheads, 1,000 Deployment Limit

United States	1000 Triad CBO	Dyad Without Bombers	Dyad Without ICBMs	SLBMs Only
GEN, LOW	820	835	800	778
GEN, ROA	572	608	729	778
DAY, LOW	585	643	507	521
DAY, ROA	387	416	485	521

Russia	Balanced Triad	No Bombers	No SLBMs	ICBMs Only
GEN, LOW	833	829	828	900
GEN, ROA	614	684	243	226
DAY, LOW	795	829	789	900
DAY, ROA	364	399	239	226

Source: As in Table 2 above.

Tables 1 through 4 show that the United States and Russia can modernize their strategic nuclear forces within New START limits on deployed weapons, or at even lower levels, while maintaining deterrence and crisis stability. Neither should be challenged to provide for assured second-strike capability, absent dramatic changes in technology favorable to defenses compared to offense; even then, pessimists can only worry about relative disadvantage in counterforce wars. There is little or no likelihood of removing populations from hostage conditions to nuclear strikes even by smaller powers, let alone the more sizable arsenals of the United States and Russia. On the other hand, by dumping New START along with the INF Treaty, Russia and the United States could bring about a new arms race that threatens the basis of nuclear-strategic stability and the continued success of the Nuclear Nonproliferation Treaty.

Russian fears that US missile defenses could nullify their retaliatory strike anticipate missile defense technologies that outperform current capabilities by a considerable margin. However, this does raise another interesting question for the United States and for Russia, with respect to "how much is enough?" when it comes to improving antimissile and air defenses. Suppose the United States and Russia push to develop defenses that *can* offer preclusive protection against nuclear attack based on current missiles and air delivered weapons. Is the resulting deterrence system more or less stable, compared

to its predecessor based on secure second-strike capability with survivable offensive weapons? Or, for a more interesting and more practical question: Would we or Russia want to develop and to deploy antimissile systems that could guarantee, say, 80 percent effectiveness against any other state's nuclear second-strike forces?

The viability of nuclear deterrence depends on cognitive simplicity and clarity with respect to the expected outcomes of any large-scale nuclear exchange. If states believe that there is no technical escape from mutual vulnerability based on secure second-strike capability, then a choice by any state for a nuclear-first strike is self-evidently pointless. However, if defenses improve to a degree sufficient to create a continuum of possible nuclear exchange outcomes, such that some outcomes are judged acceptable or tolerable compared to others ("winning ugly"), then politicians and their military advisors might mistakenly see a nuclear standoff as a competition for relative advantage, instead of a trapdoor opening the way to mutual suicide.

The preceding statement is a controversial assertion that will be disputed by those who perceive that the threat of nuclear war, as opposed to the actual decision for a nuclear attack, can be used for the manipulation of risk and for nuclear coercion short of war. This counter-argument, that nuclear ambiguity can be more useful that nuclear certainty, is situationally dependent and needs to be carefully qualified.[38] Ambiguity can be used by one state to its advantage in a coercive bargaining process, *provided* the other state can see the difference between *threats short of war* and a *decision to launch an anticipatory attack*.[39] Nuclear ambiguity may characterize a bargaining *process*, but for that process to result in an acceptable *outcome*, nuclear certainty must exist about the effects of a nuclear war.

Conclusion

The end of the INF Treaty is part of a larger problem: the need to transition to a new framework for US-Russian nuclear-strategic stability. The challenge for the Trump administration and its successors will be to manage the

38 Expert discussion of this issue appears in Todd S. Sechser and Matthew Fuhrmann, *Nuclear Weapons and Coercive Diplomacy* (Cambridge: Cambridge University Press, 2017).

39 On the problem of anticipatory attacks, see Karl P. Mueller and others, *Striking First: Preemptive and Preventive Attack in U.S. National Security Policy* (Santa Monica: RAND, 2006).

transition in three aspects: first, to maintain the cohesion of NATO and other US alliances with respect to political decision taking, military preparedness, and arms-control initiatives; second, to protect an interim level of strategic stability with Russia while a new Russian-American security framework is being created; third, to incorporate new actors, especially China, into a new framework for nuclear-strategic stability; and, fourth, to include recognition of the increased importance of new technologies, including those for the security-related uses of space, and cyber.[40]

The costs and benefits of ending the INF Treaty and jeopardizing the extension of New START are not only measured in the possibility of renewed nuclear arms race on the European continent—important as that problem is—but also in terms of the impact on the dynamics of crisis management and escalation control. Departure from the INF Treaty creates a more complicated decision space in several directions: between conventional and nuclear war; between nuclear-first use and an expanded theater-wide conflict; and, most importantly, between theater and strategic nuclear warfare. Sub-strategic nuclear weapons deployed in Europe are two faced: They are seen as deterrents by their owners, but they also invite preemptive attack on themselves at the earliest stages of a conflict. Or, if you prefer: how many Able Archers can a system withstand?[41] In addition, if a defunct INF agreement is followed by American and Russian refusals to extend the New START beyond 2021, nuclear arms control will be on a possibly irreversible descent into irrelevance. In this admittedly gloomy scenario, the Nuclear Nonproliferation Treaty may feel the tremors from the abdication by the two

40 Frank A. Rose, "The End of an Era? The INF Treaty, New START, and the Future of Strategic Stability," Brookings, February 12, 2019, https://www.brookings.edu/blog/order-from-chaos/2019/02/12/the-end-of-an-era-the-inf-treaty-new-start-and-the-future-of-strategic-stability/.

41 Able Archer 83 was a NATO command post exercise in November 1983, testing procedures for nuclear release and potential use in case of war. The exercise took place during a time of heightened US-Soviet tensions over various issues, including competing NATO and Soviet nuclear missile deployments and an ongoing Soviet KGB intelligence operation (RYAN) to detect signs of a possible NATO nuclear first strike. See Raymond L. Garthoff, *The Great Transition: American-Soviet Relations and the End of the Cold War* (Washington, DC: Brookings Institution, 1994), esp. pp. 138–139, and pertinent references therein. See also Ben Macintyre, *The Spy and The Traitor: The Greatest Espionage Story of the Cold War* (New York: Crown Publishers, 2018), pp. 142–148.

nuclear superpowers, and events may encourage other non-nuclear weapons states to reconsider their priorities.[42]

Admittedly, the challenge of keeping the INF Treaty in place is more complicated for Washington and Moscow than is the less controversial forwarding of New START. Russia's interest in deploying additional land-based medium and longer-range missiles in Europe and in the Far East reflects its perennial fear of encirclement, of additional "bracket creep" in NATO's membership, and of China's rising numbers of ballistic missiles of various ranges. Russia also fears an outbreak of next generation conventional US PGS systems supported by improved antimissile defenses, space-based weapons, and cyber threats, even though Russia is modernizing its military capabilities in all these categories.[43] The possible costs of jettisoning INF include reduced stability of the military-strategic balance of power in Europe and, along with this, an unintentional lowering of the nuclear threshold based on confusion between designed flexibility and unintended or inadvertent escalation.[44]

It would be an understatement to say that cyber and information strategies are wrapped around all the arms-control issues discussed hitherto. Nuclear-strategic stability at or below the threshold of general nuclear war requires that certain shared expectations between potential adversaries be cultivated like delicate flowers. For deterrence to hold firm, leaders must have confidence that they have an accurate understanding of their opponents' capabilities and intentions, including their theories of war and assumptions about deterrence. During the Cold War, these shared expectations developed slowly over time between the Americans and Soviets, and then among their respective alliance partners (for the most part, with unavoidable French pirouettes and Maoist disclaimers offering occasional distractions). Future frameworks for nuclear-

42 For pertinent background, see Henry D. Sokolski, *Underestimated: Our Not So Peaceful Nuclear Future* (Carlisle, PA: Strategic Studies Institute and US Army War College Press, January 2016).

43 Defense Intelligence Agency, *Russia Military Power: Building a Military to Support Great Power Aspirations* (Washington, DC: Defense Intelligence Agency, 2017).

44 For expert commentary on this issue, see the briefing by John K. Warden, "Limited Nuclear War: The 21st Century Challenge for the United States," Institute for Defense Analysis (IDA), SMA STRATCOM Speaker Series, September 12, 2018, https://nsiteam.com/social/wp-content/uploads/2018/09/Limited-Nuclear-War-brief-Warden.pdf.

strategic stability will have to work out similar protocols of reassurance with respect to nuclear deterrence and crisis management, but they will have to do so in the age of cyber. Now the very sources of information and assessment on which strategic reassurance is based are themselves in danger of deliberate or inadvertent compromise. As Sanger warns,

> Cyberweapons are entirely different from nuclear arms, and their effects have so far remained relatively modest. But to assume that will continue to be true is to assume we understand the destructive power of the technology we have unleashed and that we can manage it. History suggests that is a risky bet.[45]

As for New START, its deployment ceilings and other limitations provide sufficient numbers of survivable strategic weapons for the United States and Russia under foreseeable conditions of nuclear weapons modernization. Missile defenses, unless or until they are based on new physical principles or concepts, are unlikely to change this condition. In addition, New START also provides Washington and Moscow with transparency and verification with respect to missile and warhead deployments going forward. As for the relationship between the INF Treaty and New START, on one hand, and nuclear flexibility on the other, much is scenario dependent. The United States does not want to be in a position in which it has fewer options for escalation *and* for escalation *control* than its opponent does—for the sake of credible deterrence.[46] However, the United States and NATO do not want to allow nuclear flexibility to relax the high standards for crossing the nuclear threshold. Nor should Russia wish to do so.

45 Sanger, *The Perfect Weapon,* p. 296.

46 Russian nonstrategic nuclear weapons play an important role in Russian thinking about how to deter and defeat the West. Some Russian military planners and thinkers also have sought an additional capability for "prenuclear deterrence" based on long-range conventional strike systems. See Brad Roberts, *The Case for U.S. Nuclear Weapons in the 21st Century* (Stanford: Stanford University Press, 2018), esp. pp. 134–136.

Iranian Cyber Capabilities: Assessing the Threat to Israeli Financial and Security Interests

Sam Cohen

The Iranian government continues to develop and field an increasingly sophisticated range of cyber capabilities to support their strategic interests and to enable a variety of computer-based financial crime. These capabilities have directly and adversely impacted Israel, which has been the target of major cyberattacks either affiliated or directly orchestrated by the political leadership in Tehran. To assess this strategic threat, this article outlines the evolving objectives and characteristics of Iran's cyber activity targeting Israel, including attacks on banks, airlines, the Israel Defense Forces, and critical infrastructure. The article includes a brief overview of Iran's internet and telecommunications history and a technical assessment of government-linked advanced persistent threat (APT) groups. Ultimately, the article concludes that a deterrence-by-punishment strategy utilizing Israel's computer network attack and exploitation advantage could provide an impactful—albeit not risk free—approach to offsetting Iran's rapidly improving cyber posture.

Keywords: Cyberattack, Israel, Iran, offensive cyber strategy, threat actor, APT groups, computer network attack, computer network exploitation

Sam Cohen is currently a federal cybersecurity policy intern with the Telecommunications Industry Association (TIA) in Washington DC. The views and opinions expressed in this article are his own and do not represent or necessarily reflect those of his employer, university, or other affiliated organizations.

Introduction

Iran's cyber activities are responsible for some of the most costly, sophisticated, and well-organized computer attacks endured by the Israeli government and corporate sector. International sanctions have continued to deteriorate Iran's economy and its ability to project influence abroad, which has created a geopolitical incentive for launching offensive cyber operations and engaging in illicit behavior targeting its strategic adversary, Israel. At the same time, Israel's economy, military, and national infrastructure has become increasingly reliant on vulnerable digital systems and networks to move information and promote effective interconnectivity. Iran has exploited these vulnerabilities to oppose Israeli regional interests, all while maintaining a limited political footprint. Major Iranian attacks have exploited network vulnerabilities in critical infrastructure, targeted intellectual property (IP), and compromised computer systems within operational elements of the Israel Defense Forces (IDF).

Key Iranian cyber actors—such as the Ministry of Intelligence, the Basij Cyber Council, APT33, and Ashiyane—have demonstrated a relatively high degree of sophistication during past attacks against Israel. Furthermore, Tehran continues to consolidate and organize its national cyber resources into a strategy that actively searches for vulnerabilities within Israeli infrastructure, corporate, and military information systems (IS) to enable exploitation during peace and wartime. This paper will argue that Iran's offensive cyber strategy, combined with the technical computer advancements occurring across the country, represents a long-term strategic threat to Israeli economic and national security interests. Although Iranian nuclear and ballistic missile programs and Tehran's support for terrorism tend to drive the strategic discussion in Israel, this paper will highlight how Jerusalem must also prioritize a new discourse on Israeli offensive cyber capabilities and deterrence posture to adequately respond to the growing Iranian cyber threat.

Roadmap and Scope of Analysis

The first section of the paper will provide a brief background on Iran's computer and networking history. This section will look at the evolution of computer security know-how in Iran, such as how the population interacts with computer systems courses at universities, and how a workforce continues to be indigenously developed to support an information and communications

technology (ICT) industry and to meet the growing demand for cybersecurity professionals.

The second part of the paper will provide a brief overview of computer network attack (CNA) and computer network exploitation (CNE) to help contextualize the technical scope and objectives of certain Iranian cyber activities discussed here later.

The third section will outline the evolution of Iran's cyber strategy. This section will look at Iranian government and government-linked attacks pre- and post-Stuxnet and how command authorities, such as the Iranian Cyber Army (ICA) and the Basij Cyber Council, have ushered in a new approach to offensive cyber operations targeting Iranian adversaries, particularly Israel. This part will also outline the unique geopolitical component of Iran's offensive cyber activities. Specifically, Iran's coordinated operations in cyberspace with regional political affiliates will be examined in Case Study 1 while Iranian cyber operations during the Joint Comprehensive Plan of Action (JCPOA) negotiation and sanctions process will be assessed in Case Study 2.

The fourth section will assess the technical capabilities of key Iranian threat actors who have targeted Israel in the past. This section will not analyze all relevant actors but rather will review the most sophisticated threats in order to evaluate the cyber risk Iran poses to Israeli information systems and data networks.

The fifth and final part will identify the need for a policy shift in Israel in which Iranian cyber activity is prioritized as a strategic threat just as Jerusalem has contextualized Tehran's nuclear and ballistic missile programs. Although the immediate physical threat is difficult to compare to nuclear weapons and their delivery systems, Iranian-linked cyberattacks continue to be active and consistently damaging, posing an ongoing threat to Israel's commercial and security interests. This section will outline a possible offensive approach that Jerusalem can implement to offset the strategic risks of growing Iranian cyber capabilities.

Contemporary Computer and ICT History in Iran

As early as 1993, Massoud Saffari, head of Iran's High Council of Informatics, had begun working on a national initiative to create a dedicated data communications network using the country's existing telephone

infrastructure.[1] A few years following the launch of this initiative, Iran established its first commercial Internet Service Provider (ISP). Working with the non-profit Neda Rayaneh Institute (NRI), an affiliate of the municipal government of Tehran, the newly created ISP began offering internet access in February 1995—primarily in the national capital region. That same year, the Telecommunications Company of Iran (TCI), in collaboration with the state-controlled Telecommunication Infrastructure Company (TIC), solidified its monopoly with the purchase of international internet gateways in the country and took control of the single domestic ISP.[2]

By 1994, TCI had announced the development of a nationwide packet-switched network called IranPac.[3] A few months later, a public joint stock company called the Data Communication Company of Iran (DCI) was created to take control of IranPac and begin expanding its commercial and government usage. Although the timing is unclear, three other entities were involved in the domestic data communication market by the mid-1990s, including a private company called Pars Supaleh, the Institute for Studies in Theoretical Physics and Mathematics (IPM), and the Iranian Pek Data Outreach Center.[4]

In 1996 and 1997, DCI began to establish international connections between its growing domestic network backbone and the global internet.[5] The first key development came after DCI entered into partnership with a Canadian telecommunication company called Teleglobe, which is now VSNL International Canada. Teleglobe worked with the Luxembourg satellite company Intelsat to provide Iran with its first dedicated satellite

1 David Banisar and Patricia Melendez, "Tightening the Net Part 2: The Soft War and Cyber Tactics in Iran," *Article 19 Free Word Center: Civic Space Unit* (March 2017), p. 12, https://www.article19.org/data/files/medialibrary/38619/Iran_report_part_2-FINAL.pdf.

2 Grey E. Burkhart, "National Security and the Internet in the Persian Gulf Region," March 1988, https://web.archive.org/web/20070703041209/http://www.georgetown.edu/research/arabtech/pgi98-4.html.

3 Ibid.

4 Babak Rahimi, "Cyber Dissent: The Internet in Revolutionary Iran," *Middle East Review of International Affairs Journal* 7, no. 3 (September 2003): 2–3.

5 Open Research Network, "Iran's Telecom and Internet Sector: A Comprehensive Survey," *Network Startup Resource Center: Oregon University* 1, no. 1 (June 1999): 12–13.

uplink directly integrated with the IranPac system.[6] Soon after, DCI entered into a joint venture with the Kuwaiti Ministry of Communications and the US-based Hughes Network Systems (HNS).[7] This venture centered on DCI gaining access to two very-small-aperture terminal (VSAT) hubs in Kuwait operated by HNS, which would substantially increase the geographic area within Iran supported by a dedicated internet and data transmission service, in addition to improving internet speed nationwide. The venture would eventually expand to include the Kuwait's state-controlled company Gulfsat, which—together with HNS—provided Iran's government and commercial clients with a reliable network communication service, supporting remote connections and bridges to foreign networks, including those nodes serving European, Asian, Middle Eastern, and North African markets.[8]

Iran had prioritized a well-established national internet infrastructure and it was slowly becoming accessible to the majority of the population, although network transmission services were slow and subscription fees were prohibitively costly for the country's lower socio-economic groups. DCI aimed to have 300,000 unique government users on its network by 1998, with plans to allow the public to purchase modems for private use that same year.[9] That objective had a material impact on the internet landscape in Iran, as by 2001, Tehran alone had 1,500 active internet cafes.[10] This made Iran one of the leading countries in the Middle East in terms of the number of internet cafes per major metropolitan area. Today, the ISP market has become more diversified, with government-linked providers such as Irancell and Hamrah Aval having 67 million users, with nearly 30 million of those users having access to third or fourth generation mobile data services.[11]

A nationwide internet infrastructure and a dedicated computer industry in Iran have been active and established for at least thirty years. The presence of this telecommunication backbone and the growing commercial and private accessibility to the internet after 1998 has resulted in a computer software and hardware literate population. This is evident by the technical course

6 Ibid.

7 Burkhart, "National Security and the Internet in the Persian Gulf Region."

8 Open Research Network, "Iran's Telecom and Internet Sector: A Comprehensive Survey," 12, 15–16.

9 Rahimi, "Cyber Dissent: The Internet in Revolutionary Iran," 2–3.

10 Ibid., 4.

11 Burkhart, "National Security and the Internet in the Persian Gulf Region."

offerings that Iran's large universities provide. For example, Sharif University of Technology in Tehran has developed its own dedicated Security and Counter-Infiltration education program where undergraduate and graduate computer science students are taught fundamentals of hacking, cybersecurity, and information security policy.[12] Courses from the curriculum include Kali and Backtrack introduction to operating systems; Infiltration tests for wireless networks; SQL Injection; Infiltrating IDS and Firewall systems; and Identifying security loopholes for XSS in web based software/ applications.[13] In 2013, Iran also launched a nationwide curriculum emphasizing scripting and hacking at the high-school level.[14] FARS News Agency, an Iranian media group, announced that certain courses would center on hacking the computer systems that supported unmanned aerial vehicles (UAVs), where technically proficient computer science students are taught remote access and authorization control techniques.[15] Many of these students are directed into cybersecurity and information assurance university programs based in Tehran.

Iran's internet and data communication infrastructure expansion in the 1990s initiated the growth of a national computer security industry. Combined with growing computer course offerings at universities and the rising demand for private industry networking, coding, and data management professionals, the country's digital sophistication and the national cyber talent pool supporting attacks will likely increase. Intellectual property theft conducted by the Iranian government will also continue to have a positive influence, as foreign computer technology will allow indigenous market developments to occur at accelerated rates.

12 Banisar and Melendez, "Tightening the Net Part 2: The Soft War and Cyber Tactics in Iran," 32, 57.

13 Ibid., 58.

14 Ginger Hill, "Iran Adds Hacking to Their High School Curriculum," *Security Today*, September 4, 2013, https://securitytoday.com/articles/2013/09/04/iran-adds-hacking-to-their-high-school-curriculum.aspx.

15 Ibid; Micah D. Halpern, "Iran's Teaching Hacking in High School," *Huffington Post,* August 30, 2013, https://www.huffingtonpost.com/micah-d-halpern/iran-hacking-school_b_3836482.html.

Understanding Computer Network Attack and Exploitation

To understand how Iran has leveraged cyberspace for its geopolitical, financial, and security objectives, it is important to differentiate between different types of cyber activity. Without understanding the technical differences, it is more difficult to describe why Tehran was involved in a certain operation, which actors specifically benefited from a given attack or espionage campaign and how much technical knowledge or capability was required to launch the operation successfully. To highlight these technical differences, this section will briefly review the three primary operational components of cyber strategy or warfare: computer network exploitation (CNE), computer network attack (CNA), and computer network defense (CND)—all of which can be collectively described as computer network operations (CNO). CNO is a broad term used to describe both military and civilian computing processes that leverage digital networks and their connected information systems, assets, and data for strategic purposes. CNO enables organizations to attack and disrupt adversarial computer networks, defend friendly infrastructure connected to the internet, protect internal information systems from attack or espionage, and exploit targeted computer networks through intelligence collection.[16]

CNE is used for intelligence, surveillance, and reconnaissance (ISR) purposes to prepare for a major attack or to enable espionage activities within targeted computer systems.[17] These operations are usually conducted using tools and processes that penetrate a targeted network and then slowly search for additional security vulnerabilities to be leveraged at a later date. CNE can be a tailored operation searching for a predetermined piece of information or an operation aiming to penetrate a specific information asset—such as an employee records database or an email server distributing a network's sensitive information. When CNE activities are not tailored and are intended to be prolonged general espionage campaigns, actors will usually move throughout the targeted network by escalating user privileges, establishing

16 Clay Wilson, "Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues," *Congressional Research Service: Report for Congress—Foreign Affairs, Defense, and Trade Division* (March 2007): 5–6.

17 Kim Zetter, "Hacker Lexicon: What are CNE and CNA?" *WIRED*, July 16, 2006, https://www.wired.com/2016/07/hacker-lexicon-cne-cna/.

root or administrative level authorizations, and mapping all assets within the network to understand where relevant data is held.

CNA is defined as operations disrupting or destroying information or data processes resident in a targeted computer or being supported by a targeted network.[18] The tools used for CNA are similar to those used for computer exploitation in terms of compromising a target but configured for systems disruption rather than intelligence collection. CNA operations can be physically, financially, and strategically damaging. For example, distributed denial of service (DDoS) attacks attempt to make a network service unavailable by overwhelming it with traffic from multiple sources, which is typically facilitated by a botnet with a malicious command and control server coordinating the overall attack infrastructure.[19] This type of CNA represents more of a reputational and financial challenge for companies or governments, as a financial institution's online banking terminal or a government's social services portal may be inaccessible for a period of time. A more serious CNA can include an incident where an application containing logical malware is installed on a targeted network, which could result in major information systems becoming corrupted or data being deleted, altered, or encrypted for ransom. For example, a CNA utilizing malware that enables an attacker to have interactive remote control over an endpoint or information system can allow the attacker to signal a computer to shut off the power flow to a piece of industrial equipment, inducing a severe operating error at a critical infrastructure facility or a corporate factory.

CND is defined as defensive measures used to protect information, computers, and networks from accidental and targeted disruption, exploitation, or destruction.[20] CND can include tools that passively monitor, prevent, and respond to unauthorized computer activity, such as firewalls or adaptive data encryption, or it can include more active measures, such as monitoring adversarial computers from within to determine their capabilities and intentions or incorporating threat intelligence into corporate and government cybersecurity

18 Ibid.

19 Andrew Shoemaker, "How to Identify a Mirai-Style DDoS Attack," *Imperva Incapsula: Security Reports*, April 10, 2017, https://www.incapsula.com/blog/how-to-identify-a-mirai-style-ddos-attack.html.

20 Wilson, "Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues," 5–6.

programs.[21] A core mission of CND aims to enhance organizational information integrity while also providing sufficient response capabilities for security teams containing, eradicating, and recovering from cyber incidents.

Evolution of Iranian Cyber Strategy and Command Authorities

During a 2015 interview with Iranian media outlet *Defa Press*, Behrouz Esbati, the commander of Iran's General Staff Cyber Headquarters (GSCH) stated that "cyber security and capabilities are no less important than the nuclear issue."[22] This comment summarizes the high-level strategic importance that Tehran has placed on being able to defend and attack through digital networks. Although certain hacking groups within Iran can be traced to domestic political attacks in the early 2000s, the emergence of government-linked operations specifically targeting foreign adversaries first appeared in 2007 when the Islamic Revolutionary Guard Corps (IRGC) established the Center for the Study of Organized Crime.[23] Intelligence and government officials in the West have classified this organization as Iran's first government coordinated hacking group and, with that, Iran's first official commitment to an offensive effort in cyberspace. By 2009, the IRGC began recruiting professionals for its internal cyber force and the closely linked military unit called the Iranian Cyber Army (ICA).[24] Furthermore, IRGC Commander Hossein Hamedani

21 James Mulvenon, "The PLA and Information Warfare," in *The People's Liberation Army in the Information Age*, ed. James C. Mulvenon and Richard H Yang (Santa Monica, CA: Rand Corporation, 1999), pp. 185–186; Larry Hollingsworth, "Blacking Threats With CND: Protect Your Network From Hackers & Attackers," *MIL Corporation*, June 2018, https://www.milcorp.com/service-areas/cyber-security/computer-network-defense/.

22 Paul Bucala and Caitlan Shayda Pendleton, "Iranian Cyber Strategy: A View from the Iranian Military," *American Enterprise Institute: Critical Threats Project* (November 24, 2015), p. 7, https://www.criticalthreats.org/analysis/iranian-cyber-strategy-a-view-from-the-iranian-military.

23 Colin Anderson and Karim Sadjadpur, "Iran's Cyber Threat: Espionage, Sabotage and Revenge," *Carnegie Endowment for International Peace* (January 4, 2018), pp. 10–11, 60, https://carnegieendowme nt.org/2018/01/04/iran-s-cyber-threat-introduction-pub-75138.

24 Ashley Wheeler, "The Iranian Cyber Threat," *Phoenix TS: Tech Roots Project*, September 12, 2013, https://phoenixts.com/blog/the-iranian-cyber-threat-part-1-irans-total-cyber-structure/; Banisar, "Tightening the Net Part 2: The Soft War and Cyber Tactics in Iran," 7.

announced in 2010 that the Basij Cyber Council—an additional cyber entity under the IRGC—had trained 1,500 cybersecurity professionals to deploy as part of its growing offensive attack and espionage outfit.[25] In 2009, leaders of this Basij cyber unit specifically called for digital attacks "against the actions of the Zionist Entity [Israel]."[26]

In 2010, Israel and the United States launched a malicious computer worm targeting Iran's nuclear program. The worm was called Stuxnet and its advanced payload utilized four different zero-day exploits affecting Windows Operating Systems (OS) and Siemens industrial control software.[27] The worm spread throughout commercial and government information systems (IS) and endpoints before eventually reaching critical nodes within Supervisory Control and Data Acquisition (SCADA) systems at Iranian nuclear production facilities. Stuxnet compromised key programmable logic controllers (PLCs) that operated the industrial equipment at these nuclear sites, which resulted in the destruction of 984 centrifuges and other machines that Iran was using to enrich uranium for an alleged weapons program.[28] Similar joint US-Israeli industrial control system attacks would occur in the following years, with the modular FLAME and WIPER variant malwares attacking PLCs at Iranian oil and natural gas production facilities and other elements of the country's critical infrastructure—such as the national financial transaction system.[29]

Iran perceived Stuxnet and similar follow-on attacks as a demonstration of how their adversaries were weaponizing cyberspace and exploiting underlying weaknesses within the country's digital security apparatus. Tehran's initial response was defensive, aiming to prevent and mitigate the network vulnerabilities that allowed Stuxnet, FLAME, and WIPER variants to be successful. For example, after the 2010 Stuxnet attack, Iran created the Cyber Defense Command and a new cybersecurity department under

25 Michael Connell, "Deterring Iran's Use of Offensive Cyber: A Case Study," *CNA Analysis and Solutions and Defense Technical Information Center (DTIC)*, October 2014, https://apps.dtic.mil/dtic/tr/fulltext/u2/a6 17308.pdf.

26 Banisar, "Tightening the Net Part 2: The Soft War and Cyber Tactics in Iran," 33.

27 Kim Zetter, "An Unprecedented Look at the World's First Digital Weapon," *WIRED: Security Reports*, November 3, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

28 Ibid.

29 Elinor Mills, "Behind the 'Flame' Malware Spying on Mideast Computers," *CNET*, June 4, 2012, https://www.cnet.com/news/behind-the-flame-malware-spying-on-mideast-computers-faq/.

the Passive Defense Organization (PDO) to protect domestic information systems from foreign adversaries infiltrating key networks.[30] However, Tehran also initiated a dramatic reorientation of its offensive cyber posture by directing its intelligence, security, and private industry resources to target and infiltrate adversarial networks. This was a strategic shift that emphasized not only computer-based financial crime and intellectual property (IP) theft to support the country's economy but also the leveraging of cyberspace as a new national tool for achieving geopolitical objectives.

Although an emphasis on offensive cyber capabilities and activity does not impact only Israel's economic and security interests, since Saudi Arabia, the United States, and other European and Middle Eastern powers are also considered adversaries of Tehran, it is clear that Iranian hacking groups have prioritized Israel as a prime target. For example, a 2014 CNE campaign called Operation Newscaster and a 2014 CNA campaign called Thamar Reservoir were both Iranian operations that had unique tactics, techniques, and procedures (TTPs) targeting Israeli government and military officials.[31] The security firm ClearSky Cybersecurity conducted a quantitative assessment of Thamar Reservoir and found that Israel was subjected to 14 percent of all the attacks and social engineering operations that were launched and represented the second largest targeted country after Saudi Arabia. The United States, Britain, Canada, and other Western countries all were subjected to fewer than 3 percent each of the overall coordinated Iranian effort.[32] Similar ratios were also identified during Operation Newscaster. These figures reinforce the notion that while Iran's offensive strategy has multiple objectives and targets, Israeli information systems have been labeled as a key strategic priority.

---

30 Banisar, "Tightening the Net Part 2: The Soft War and Cyber Tactics in Iran," 8; Connell, "Deterring Iran's Use of Offensive Cyber: A Case Study," 4.

31 ClearSky Research Team, "Thamar Reservoir: An Iranian Cyber-Attack Campaign against Targets in the Middle East," *ClearSky Cybersecurity, Inc.*, June 2015, https://www.clearskysec.com/wp-content/uploads/2015/06/Thamar-Reservoir-public1.pdf; Jim Finkle, "Iranian Hackers use Fake Facebook Accounts to Spy on U.S., Israel and others," *Reuters*, May 29, 2014, https://www.reuters.com/article/iran-hackers/iranian-hackers-use-fake-facebook-accounts-to-spy-on-u-s-others-idUSL1N0OE2CU20140529.

32 ClearSky Research Team, "Thamar Reservoir," 12.

Case Study 1: Regional Threat Actor Affiliates

In the years following the 2010 Stuxnet attack, Iranian officials began to aggressively leverage Israeli vulnerabilities in cyberspace. This included cooperation with Hamas and Hezbollah hacking groups who, together with Iran, conducted CNA and CNE operations against the Israeli Security Agency (Shin Bet), Home Front Command, the Office of the Prime Minister, the Defense Ministry, Bank of Jerusalem, El Al Airlines (Israel's national airline), Likud and Kadima Political Parties, and operational components of the IDF.[33] Other Iranian computer attacks have attempted to infiltrate local area networks (LANs) of "vital national systems" according to a 2013 statement by Israel's Prime Minister Benjamin Netanyahu.[34] His statement noted that Iran had begun targeting water, power, and financial transaction infrastructure, in addition to social service websites operated by the government.

According to an article in the *Jerusalem Post*, one of Hamas' preeminent hackers, Maagad Ben Juwad Oydeh, successfully infiltrated IDF data communications networks and routed data downlinks from IDF drones hovering over Gaza to Hamas commanders.[35] Beginning in 2012, the commanders had a direct real-time feed of aerial surveillance videos that were being relayed from Israeli unmanned aircraft. By 2015, Oydeh was able to extract the global positioning system (GPS) signals from the drones he was targeting, which allowed senior Hamas militants to maneuver forces and weapons away from monitored areas.[36] Israeli security forces arrested and in 2016 convicted Oydeh on charges of spying, conspiracy, contact with enemy agents, and membership in an illegal organization.

Iran has also worked with Hamas to support their cyber operations aiming to disrupt Israeli military and political activities in Gaza. For example, during the 2012 Hamas war, Israel faced a sophisticated cyber campaign

33 Gabi Siboni, Matthew Cohen, and Charles Freilich, "Israel and Cyberspace: Unique Threat and Response," *International Studies Perspectives* 17, no. 3 (August 2016): 309–310.

34 Jeffrey Heller and Maayan Lubel, "Iran Ups Cyber Attacks on Israeli Computers: Netanyahu," *Reuters*, June 9, 2013, https://www.reuters.com/article/us-israel-iran-cyber/iran-ups-cyber-attacks-on-israeli-computers-netanyahu-idUSBRE95808H20130609.

35 Yonah Jeremy, "Islamic Jihad Member Convicted In Plea Bargain For IDF Drones," *Jerusalem Post*, January 2017, https://www.jpost.com/Israel-News/Islamic-Jihad-member-convicted-in-plea-bargain-for-hacking-IDF-drones-480092.

36 Ibid.

seeking to disable government websites and operations at private financial institutions, including a national bank that was targeted by a successful DDoS attack associated with known Iranian server infrastructure.[37] There were also incidents during Israel's 2014 campaign against Hamas, where the IDF's homeland security division experienced a temporary information system breach when the Syrian Electronic Army—an Iranian-linked hacking affiliate—was able to compromise the IDF's website and temporarily upload political messages defaming ongoing Israeli operations.[38]

Another example of Iranian coordination with regional geopolitical allies is Tehran's relationship with the Hezbollah Cyber Army (HCA). The Israeli-based cyber threat intelligence firm Check Point Software Technologies attributed a series of corporate and government breaches across Israel's defense sector from 2013 to 2015 to the HCA.[39] The group's campaign—called Volatile Cedar—was relatively advanced, well planned, and the attackers were patient while scanning for external network vulnerabilities as to limit their exposure. A custom malware variant, referred to as EXPLOSIVE, acted as a Trojan program allowing the attackers to establish remote interactive control over externally facing servers and information systems. The attackers then used these compromised assets to pivot toward internally facing servers where they could deploy other modules of the malware on network hosts.[40] The malware's technical features indicate that it was developed by Iran and subsequently distributed to the HCA, which is consistent with the overall trend of Iranian cyber authorities disseminating training and technical resources to Hezbollah-linked threat actors.[41]

In addition to foreign affiliates, Tehran has also utilized part-time domestic private hacking groups for less sophisticated cyber operations that are aligned

37 Siboni, Cohen and Freilich, "Israel and Cyberspace: Unique Threat and Response," 312.

38 Ibid.

39 Ben Shaefer, "The Cyber Party of God: How Hezbollah Could Transform Cyberterrorism," *Georgetown Security Studies Review*, March 11, 2018, http://georgetownsecuritystudiesreview.org/2018/03/11/the-cyber-party-of-god-how-hezbollah-could-transform-cyberterrorism/.

40 Threat Intelligence and Research Team, "Volatile Cedar," *Check point Software Technologies*, pp. 1–2, March 30, 2015, https://www.checkpoint.com/downloads/volatile-cedar-technical-report.pdf.

41 Anderson and Sadjadpur, "Iran's Cyber Threat: Espionage, Sabotage and Revenge," 21.

with the country's foreign policy objectives. For example, in 2018 a private group called Charming Kitten was responsible for conducing Man-In-The-Browser attacks utilizing a browser exploitation framework (BEF) against multiple Jewish media outlets inside the United States who were supporters of Israel.[42] Similar attacks have also occurred against the American Israel Public Affairs Committee (AIPAC), Jewish political and academic leaders around the world, and organizations supportive of Israeli actions in Gaza or Lebanon.[43]

Case Study 2: JCPOA and an Adapting Iranian Cyber Strategy

The use of offensive cyber activity as a response mechanism to regional security developments has been a frequent policy option pursued by Tehran, specifically to counter Israeli interests. Based on the previous examples analyzed, it is clear that Iran routinely coordinates cyber operations with regional security partners to launch integrated and tailored attacks against Israeli commercial and government institutions. These attacks and espionage campaigns tend to occur during periods of security activity in the region, such as Israeli incursions into Gaza or Lebanon. This trend indicates that Iranian offensive cyber activity is intricately linked and constantly adapting to the country's geopolitical interests at any given time. This strategic approach is not necessarily an underlying characteristic of the cyber policies of other countries, such as Russia or China. For example, Moscow and Beijing, who both have access to a talent pool and technical infrastructure that greatly exceeds the sophistication of training, resources, and capability in Iran, can be described as constant systemic actors routinely launching attacks regardless of geopolitical conditions.[44] While that is true for certain cyber actors focused on financial crime in Iran, those groups tend to be less controlled and unaligned with government policy priorities, such as the independent Iranian hackers responsible for the HBO breach in 2015 after the JCPOA

42 Oded Yaron, "Iranian Hackers Tried to Impersonate Israeli Cyber-Security Company," *Haaretz*, July 9, 2018, https://www.haaretz.com/israel-news/premium-iranian-hackers-break-into-israeli-cybersecurity-site-1.6263629.

43 Anderson and Sadjadpur, "Iran's Cyber Threat: Espionage, Sabotage and Revenge," 35.

44 Mark Pomerleau, "DoD Releases First New Cyber Strategy in Three Years," *The Fifth Domain,* September 18, 2018, https://www.fifthdomain.com/dod/2018/09/19/department-of-defense-unveils-new-cyber-strategy/.

agreement was signed and international sanctions were lifted.[45] The regular changes in the frequency of Iranian CNA and CNE is uncharacteristic of Chinese and Russian threat actors and highlight the uniqueness of the Iranian threat to Israel as it is fundamentally strategic and long term.

The pattern of Iranian cyber activity closely adjusting to an evolving geopolitical development has been evident throughout the JCPOA negotiation and sanctions process. US government officials have noted that in the period leading up to the negotiations in 2013 and 2014, Iran was conducting major cyber operations that caused significant financial damage to companies throughout the West and the Middle East, including in the United States, Canada, Britain, Israel, Saudi Arabia, and even Turkey.[46] Following the large-scale operations, US Attorney General Loretta Lynch stated, "These attacks were relentless, they were systematic, and they were widespread."[47] Michael Daniel, president of the Cyber Threat Alliance, explained in 2017 that "once Iran decided it really wanted to come to the table and actually negotiate something serious, they naturally took steps in a whole variety of areas to ramp back activities so that they weren't being so confrontational."[48] Iran significantly increased its offensive cyber activity during the sanctions period leading up to negotiations while it very rapidly deescalated that same policy once the deal neared agreement. It is clear that a change in geopolitical conditions between 2014 and 2015 induced the rollback of Tehran's aggressive cyber campaign during the previous two years. Levi Gundert, an Iran-focused analyst at the private intelligence firm Recorded Future noted, "Most of the destructive attacks were pre-2015. Then we had the Iran nuclear deal."[49]

---

45 Andy Greenberg, "The Iran Nuclear Deal's Unraveling Raising Fears of Cyber Attacks," *WIRED*, May 9, 2018, https://www.wired.com/story/iran-nuclear-deal-cyberattacks/.

46 Kate Brannen, "Abandoning Iranian Nuclear Deal Could Lead to New Wave of Cyber Attacks," *Foreign Policy*, October 2, 2017, https://foreignpolicy.com/2017/10/02/abandoning-iranian-nuclear-deal-could-lead-to-new-wave-of-cyberattacks/.

47 Dustin Voltz, "U.S. Indicts Iranians for Hacking Dozens of Banks, New York Dam," *Reuters*, March 24, 2016, https://www.reuters.com/article/usa-iran-cyber/u-s-indicts-iranians-for-hacking-dozens-of-banks-new-york-dam-idUSL2N16W1I4.

48 Brannen, "Abandoning Iranian Nuclear Deal Could Lead to New Wave of Cyber Attacks."

49 Greenberg, "The Iran Nuclear Deal's Unraveling Raising Fears of Cyber Attacks."

While negotiations and official agreement in 2015 curbed Iranian cyber activities targeting its adversaries, President Trump's decision to officially withdraw from the JCPOA nuclear deal in May 2018 had the opposite affect. The computer security firm CrowdStrike released a report identifying a notable shift in activity associated with Iranian hacking groups, just twenty-four hours after Trump's May withdrawal announcement.[50] The activity included spear-phishing operations that had been designed with social engineering efforts, containing malicious email attachments that were tailored to breach pre-selected corporate and government cybersecurity programs. The emails were mainly delivered to US commercial executives and military officials, but the report indicates that senior military and political representatives of other US allies, such as Israel, had been specifically targeted abroad.[51] The extensive preparation that had gone into the attack suggests that Tehran was timing the operation as a geopolitical response to Trump's official statement, which reinforces the notion of Iran's offensive cyber strategy being tethered to their fluctuating strategic objectives and national security priorities.

Iran has yet to publish a comprehensive single document that outlines its overall cyber strategy or its objectives, targets, policies, and methods for offensive operations. However, official public statements from the Iranian government combined with attributed Iranian-linked CNA and CNE, which have specifically sought to exploit vulnerabilities in Israel and its allies, demonstrate how the country has moved away from its largely defensive and pre-Stuxnet cyber posture. For example, Frank Cilluffo, director of Center for Cyber and Homeland Security, stated in 2017 that "In recent years, Iran has invested heavily in building out their computer network attack and exploit capabilities. Iran's cyber budget had jumped twelvefold under President Rouhani, making it a top five cyber-power. They are also integrating cyber

50 Nicole Perlroth, "Without Nuclear Deal, U.S. Expects Resurgence in Iranian Cyberattacks," *New York Times*, May 11, 2018, https://www.nytimes.com/2018/05/11/technology/iranian-hackers-united-states.html.

51 Ibid; Zack Whittaker, "Iran likely to Retaliate with Cyberattacks after Nuclear Deal Collapse," *ZDNet*, May 9, 2019, https://www.zdnet.com/article/iran-poised-to-launch-cyberattacks-after-nuclear-deal-collapses/.

operations into their military strategy and doctrine."[52] This new emphasis on an offensive strategy, combined with declining security relations between Tehran and Jerusalem, has propelled Iranian cyber activities to the forefront of Israel's strategic threat landscape.

Iran's Technical Cyber Capabilities: Analyzing Key Threat Actors

It is important to review the sophistication of key Iranian threat actors to determine the technical and policy risks facing Israel. Although only a small portion of the Iranian cyber landscape will be analyzed, this section will still highlight how Iran's most experienced cyber professionals are rapidly improving their technical knowledge to support offensive behavior—including attacks targeting Israeli infrastructure, military, and commercial information systems.

First discovered by US cybersecurity firm FireEye, APT33 is an Iranian hacking group responsible for an array of breaches across infrastructure, banking, aerospace and petrochemical industries in Israel, the United States, the United Kingdom, South Korea, and Saudi Arabia.[53] An advanced persistent threat (APT) is a malicious computer attack where a person or group gains unauthorized access to a network and remains undetected for an extended period, usually mapping the network for additional vulnerabilities, escalating their user privileges, or uploading backdoors to enable remote interaction. APTs have traditionally been associated with nation-state actors due to the financial resources, talent, and infrastructure that usually support their operations, which accurately describes APT33's relationship with the Iranian government. FireEye and the Russian-based cybersecurity firm, Kaspersky Lab, have both released reports detailing the intricate connections between APT33 and the Iranian government's Nasr Institute, which is a contractor jointly operated by the IRGC's Basij cyber unit and the Ministry

52 Eric Auchard, "Once 'Kittens' in Cyber Spy World, Iran Gains Prowess: Security Experts," *Reuters*, September 20, 2017, https://uk.reuters.com/article/us-iran-cyber/once-kittens-in-cyber-spy-world-iran-gains-prowess-security-experts-idUKKCN1BV1VA.

53 Thomas Brewster, "Meet APT33: A Gnarly Iranian Hacker Crew Threatening Destruction," *Forbes*, September 20, 2017, https://www.forbes.com/sites/thomasbrewster/2017/09/20/iran-hacker-crew-apt33-heading-for-destructive-cyberattacks/#5b5693174a48.

of Intelligence.[54] US and Israeli government reports also indicate that many of the personnel believed to be associated with APT33 previously have worked in other Iranian hacking groups and within the Iranian government itself.

Although APT33 is not dedicated to only attacking Israel, it has conducted highly tailored and complicated operations that have disrupted and damaged Israeli information systems. The group routinely uses a complex Trojan program called DROPSHOT, which allows malware to bypass anti-virus systems and execute non-malicious programs in virtual sandbox environments to avoid detection by security teams.[55] The malware is believed to be a derivative of similar code used by another advanced Iranian hacking group called the Sword of Justice, which was responsible for developing and launching the highly capable and damaging Shamoon malware in 2012.[56] APT33 has also included new versions of NANOCORE and NETWIRE remote access trojans (RATs) as payloads for their DROPSHOT tool, which has provided the group with a full-spectrum capability to enter protected systems, locate additional vulnerabilities, extract or delete data, and remove evidence from operational and security logs.[57] This has made attribution and root cause analysis with APT33 attacks extremely difficult, which, in turn, has hindered countermeasure development for the group's operations.

APT33 is an example of one of Iran's most advanced malicious cyber groups who routinely conducts CNA and CNE operations against adversaries. The group's activity has been at the forefront of Iran's offensive cyber strategy and has had direct military impact on Israel. For example, during the 2014 Israel-Gaza war, it is believed that APT33 was behind a breach of a civilian-military communication network distributing battlespace intelligence.[58]

54 Jacqueline O'Leary, Josiah Kimble, and Kelli Vanderlee, "Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and Has Ties to Destructive Malware," *FireEye: Threat Research Team*, September 20, 2017, https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html.

55 Ibid.

56 Andy Greenberg, "New Group of Iranian Hackers Linked to Destructive Malware," *WIRED*, September 20, 2017, https://www.wired.com/story/iran-hackers-apt33/.

57 O'Leary, Kimble, and Vanderlee, "Insights into Iranian Cyber Espionage: APT33."

58 Yaakov Lappin, "Iran Attempted Large-Scale Cyber Attack On Israel, Senior Security Source Says," *Jerusalem Post*, August 17, 2014, https://www.jpost.com/Arab-Israeli-Conflict/Iran-attempted-large-scale-cyber-attack-on-Israel-senior-security-source-says-371339.

Private security firms have linked APT33 to the attacks due to the TTPs and malware variants used during the operation. The compromised network, however, only experienced a short period of data relay disruptions between command and control entities, which resulted in an extremely minor impact on the overall war effort.[59] Although the attack was not entirely successful, it demonstrates how Iran is creating the technical capability to induce real costs to IDF operations and Israeli military posture.

There are also advanced Iranian threat actors inducing significant financial harm to Israel and affecting its economic interests. For example, an Iranian APT called COBALT DICKENS conducted a CNA operation in 2018 targeting research institutes, universities, and professors around the world.[60] Over fifteen billion pages of intellectual property (IP) were stolen from the databases and information assets of facilities in twenty-two different countries. Security firms estimate that the IP is worth 3.4 billion dollars.[61] Universities in Israel were successfully targeted during this operation, although the exact losses suffered by specific universities have not been made public.[62] COBALT DICKENS has also been identified as a partner group to the Iranian Mabna Institute, who has strong ties to another Iranian-linked firm called the Nasr Institute. These groups have been linked to DoS and other computer attacks on Israeli banks, in addition to stealing trade secrets from Israeli and allied companies.[63]

---

59 Ibid.

60 John Kuhn, "COBALT DICKENS Targets Universities," *IBM X-Force Threat Exchange*, August 29, 2018, https://exchange.xforce.ibmcloud.com/collection/COBALT-DICKENS-Targets-Universities-4bdbb7eff5196b24ce4981abcffec11e.

61 Victoria Bekiempis and Larry McShane, "Iranian Hackers Stole $3.4B in Intellectual Property from Hundreds of Universities across the World," *NY Daily News*, March 23, 2013, https://www.nydailynews.com/news/crime/iran-hackers-breached-5-u-s-gov-computer-systems-prosecutors-article-1.3891703.

62 "Israeli University Compromised in Iran Hack," *Times of Israel*, March 24, 2018, https://www.timesofisrael.com/israeli-university-accounts-compromised-in-iran-hacking-scheme/.

63 Pierluigi Paganini, "Iran-linked COBALT DICKENS Group Targets Universities in New Phishing Campaign," *Security Affairs*, August 28, 2018, https://securityaffairs.co/wordpress/75710/cyber-warfare-2/cobalt-dickens-iran-attacks.html; Charlie Osborne, "Iranian Hackers Target 70 Universities Worldwide to Steal Research," *ZDNet*, August 24, 2018, https://www.zdnet.com/article/iran-hackers-target-70-universities-in-14-countries/; Brewster, "Meet APT33: A Gnarly Iranian Hacker Crew Threatening Destruction."

Another APT group that has specifically targeted Israel and has been a generally active component of Iran's offensive cyber strategy is OilRig. Initially active in 2015, OilRig has conducted successful spear phishing and domain name system (DNS) spoofing attacks against multiple law firms, banks, and third-party information technology (IT) vendors that serve the financial industry in Israel.[64] Although the metrics of these attacks and resulting financial costs are extremely vague and underreported, Israeli media and government statements indicate that certain attacks have compromised critical payment card industry (PCI), market trading, and index reporting information systems. Palo Alto Networks reported that OilRig also successfully attacked financial institutions and technology organizations within Saudi Arabia.[65]

OilRig is an example of an increasingly capable Iranian threat actor. One of the TTPs the group utilizes involves sending malicious Microsoft Excel attachments to an employee at the target organization. Once the employee opens the attachment, the file displays decoy content within the spreadsheet and installs a variant of HELMINTH malware. This malware opens up a backdoor linking the endpoint to a command and control server, which then provides the group with remote functional control of the infected endpoint.[66] The attackers have also used advanced obfuscation techniques to mask their attack infrastructure and certain details of the HELMINTH malware itself, which has impeded security investigations and created challenges for corporate cybersecurity programs in Israel's financial industry.

The last actor that is important to the technical assessment of Iranian cyber capabilities is the Ashiyane Digital Security Team, also referred to as Ashiyane or NEST. Ashiyane is a unique actor within the overall Iranian threat landscape as, in addition to their malicious operations, they also act as one of the largest online educational and training resources for the

64 ClearSky Research Team, "Iranian Threat Agent OilRig Delivers Digitally Signed Malware, Impersonates University of Oxford," *ClearSky Cybersecurity Inc.*, January 5, 2017, https://www.clearskysec.com/oilrig/.

65 Robert Falcone and Bryan Lee, "The OilRig Campaign: Attacks on Saudi Arabian Organizations Deliver Helminth Backdoor," *Palo Alto Networks*, May 26, 2016, https://researchcenter.paloaltonetworks.com/2016/05/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/.

66 Ibid.

hacking and computer security community in Iran.[67] For example, members of Ashiyane have attended hackathons and security conferences in Qom as keynote speakers.[68] During closed seminars at these events, members of the group review TTPs for Linux server infiltration, DDoS operations, and SQL Injection attacks. As of 2017, there were allegedly 363,949 unique members participating in the group's online tutorials, which ranged from instructional videos and interactive labs focusing on Access Control, Privilege Escalation, OS Analysis and Scanning, Network Management and Infiltration, Cryptography, Email Security, and RAT Development.[69]

Ashiyane's malicious CNA and CNE activities are not as advanced, dedicated, or resource intensive as other major threat actors such as APT33. In 2017, cybersecurity firms attributed to Ashiyane the defacement and service interruption of 500 Israeli and other Western websites during the 2009 Israeli incursion into Gaza.[70] The group was also responsible for widespread DDoS attacks that targeted 1,000 websites in the United States, Britain, and France in 2010 for supporting anti-Iranian activist groups.[71] Although these operations have been politically and financially impactful, their technical sophistication has not been similar to Iran's predominant threat actors. However, since the group is the most technically proficient and up-to-date educational resource for hackers within the country, it is clear that Ashiyane has been a major facilitator of the growing Iranian offensive cyber threat through their training and lab-based education network. The Iranian government itself has recognized the impact the group has had within the hacking community, with entities such as the Grand Ayatollah Makarem Shirazi—a Shiite religious authority—the FATA Police and leaders within the IRGC praising their work.[72]

---

67 Dorothy Denning, "Following the Developing Iranian Cyberthreat," *Scientific American*, December 12, 2017, https://www.scientificamerican.com/article/following-the-developing-iranian-cyberthreat/.

68 Banisar and Melendez, "Tightening the Net Part 2: The Soft War and Cyber Tactics in Iran," 34.

69 Ibid.

70 Denning, "Following the Developing Iranian Cyberthreat."

71 Ibid.

72 Banisar and Melendez, "Tightening the Net Part 2: The Soft War and Cyber Tactics in Iran," 34.

Although the sophistication of the actors discussed in this section represent the minority of the overall Iranian threat landscape, it is clear that certain groups linked to the Iranian government or working for the government directly are becoming increasingly advanced. Further, the scale, complexity, and scope of the 2018 COBALT DICKENS attack—although not solely aimed at Israeli institutions—demonstrated how Iran's overall cyber ambitions are rising concurrently with the nation's technical capabilities and resources. The specific economic and military objectives of future Iranian offensive operations will likely adapt and evolve as key threat actors become more technically proficient, but the general aim of using cyberspace as a strategic tool to pressure Israel will remain constant.

Strategic Policy Shift: Offsetting the Iranian Cyber Threat

Rapid digitalization of critical infrastructure and the increasing use of susceptible information and communications technology (ICT) throughout Israel has created a large attack surface vulnerable to Iranian threat actors. In 2011, Israel's Prime Minister Benjamin Netanyahu told a Tel Aviv cybersecurity conference, "The more computerized we get, the more vulnerable we become. There is therefore no choice but to deal with this in a more systematic and focused manner."[73] At the same conference the Israeli Security Service's Cyber Task Force chief stated that "Israeli networks critical to communications, transport systems, finance, and the supply of electricity and water are all wide open to attack. This constitutes a major threat to national security."[74] These comments indicate that a strategic perspective of cyberspace had already been active in Israel for several years. For example, major policy reforms in 2015 strengthened the roles and capabilities of the National Cybersecurity Authority, the National Cyber Directorate, the Information Security Agency, and the now terminated Cyber Command project.[75] However, in 2016, Israel's Energy Authority responsible for national electric grids still experienced

73 Matthew Kalman, "Israel Vulnerable To Cyber Attack, Leaders Warn," *MIT Technology Review*, June 15, 2011, https://www.technologyreview.com/s/424302/israel-vulnerable-to-cyber-attack-leaders-warn/.

74 Ibid.

75 Deborah Housen-Couriel, "National Cyber Security Organization: Israel," C*yber Defense Center of Excellence NATO* 2, no. 4 (February 2017): 11–12.

a two-day information system shutdown after a systemic APT attack.[76] Regardless of the commitment to cybersecurity expressed in 2011 by the prime minister, this attack indicates that the threat to the country has only worsened and that previous responses have failed to mitigate the technical and strategic cyber threat.

An underlying feature of why a traditional detection and protection approach will not address evolving Iranian capabilities and intent is due to the geopolitical nature of the threat. For example, Russia is a financially motivated cyber actor in Israel, primarily conducting intellectual property (IP) theft, identity fraud, and computer-based transaction crime.[77] Adding barriers to Russian cyber operations with a computer network defense (CND) strategy reduces the financial return Russian actors receive due to the additional time, talent, and technical costs that would need to be put into attack preparation and execution. Alternatively, Iran's cyber motivations in Israel are largely strategic and geopolitically driven. Although there are numerous instances of Iranian actors, such as COBALT DICKENS, focusing on financial and IP objectives, the threat landscape is overwhelmingly targeted at Israeli security and economic interests that hurt and pressure the Israeli government at a strategic level—not at a specific company level—and not necessarily to the financial benefit of Tehran. Although a deterrence-by-denial strategy seeking to leverage Israel's advanced cybersecurity industry is useful to ensure less sophisticated Iranian groups are not incentivized to target Israel, Jerusalem must also develop and implement a cyber centric deterrence-by-punishment strategy.

The key aspect of a deterrence-by-punishment strategy is that it threatens unacceptable costs in response to an adversary's first strike action, or in this case, a major Iranian CNA or espionage campaign. The massive reorientation of Iran's cyber forces after the 2010 Stuxnet attack indicates that Tehran is likely to view an openly communicated deterrence-by-punishment strategy from Jerusalem as a highly credible strategic threat to Iranian interests—including the integrity of its energy infrastructure, military apparatus, and commercial enterprises. Further, the WIPER variants and FLAME attacks

76 Danna Harman, "Israel's Electrical Grid Targeted by 'Severe Cyberattack'" *Haaretz*, January 26, 2016, https://www.haaretz.com/israel-news/.premium-israel-s-electrical-grid-targeted-by-severe-cyberattack-1.5396042.

77 Ronen Bergman, "Israel is under Massive Chinese, Russian Cyber Espionage Attack," *Ynet*, July 31, 2018, https://www.ynetnews.com/articles/0,7340,L-5320392,00.html.

that followed Stuxnet reinforced the notion that Israel maintains a clear qualitative edge in offensive cyber activities over Iran. Israel would likely reduce the cyber risk stemming from Iran if a publicly communicated—non-covert—retaliatory policy was enacted as a guaranteed reprisal for major cyberattacks launched by Iranian groups.

Focusing on a strictly denial strategy will have a minimal impact on the geopolitical imperative that Tehran has placed on cyber operations targeting Israel. For example, Israel will never be able to completely rid its national infrastructure, military, or key commercial entities from cyber risk, which means that Tehran will always be committing financial, technical, and talent resources to search for vulnerabilities and create exploits—regardless of the cost. Although it is important for Israel to leverage its national cyber talent and cybersecurity industry to protect against non-strategic threats from other countries, such as Russia and less experienced attackers within Iran itself, a new offensive strategy is required for Jerusalem to mitigate the capability improvements Iran continues to experience. This cyber-based deterrence-by-punishment approach would be the most direct, financially conservative, and sustainable model for Israel to offset Iran's strategic objectives in cyberspace.

Outsourcing in Intelligence and Defense Agencies: A Risk of an Increase in the Proliferation of Cyber Weapons?

Omree Wechsler

The many cases of the leakage of classified materials belonging to intelligence and defense agencies have led to claims that contract workers are the reason for these incidents, due to either their lack of loyalty or negligence. In addition, these leaks of classified information, including hacking programs and components, have raised the question of whether this internal threat is also the cause of the increased proliferation of sophisticated cyber weapons among players who do not have the ability to develop them. A prominent case study from the past few years is the leak of the National Security Agency (NSA)'s hacking component, EternalBlue, and its use in the global cyberattack WannaCry, which damaged computers in 150 countries and was attributed to North Korea. Understanding the internal threat and its connection to the proliferation of cyber weapons, along with enumerating the advantages and disadvantages of hiring contractors, is critical for minimizing the threat, coping with it, and in preventing harm to national security and further deterioration of stability in cyberspace.

Keywords: Outsourcing, proliferation of cyber weapons, intelligence, contractors, information security

Omree Wechsler is head of Cyber Research at the Yuval Ne'eman Workshop for Science, Technology, and Security and at the Blavatnik Inter-Disciplinary Cyber Research Center at Tel Aviv University.

Introduction

Much has been said about the disadvantages of outsourcing and privatizing of non-cybernetic security functions and services, which include problems of ethics and accountability when transferring the authority to use force into the hands of private companies. A number of leaks of classified materials, some of which have included source code of hacking tools, have led US senior officials to express the dangers of hiring contract workers in sensitive security industries, including the cyber industry.

After the Vault 7 leak, which included source codes of a CIA hacking tools, Director of the CIA and American Defense Secretary Leon Panetta said that employing contract workers carried risks, and that it was possible that they did not have the same loyalty to the organization that the agency's permanent employees had.[1] After another leak, Republican Senator Ben Sasse claimed that the NSA had to solve the problem of the leaks, the source of which was the agency's contractors.[2] These statements suggest that contract employees at American intelligence agencies are considered more problematic than permanent government employees.

The use of contractors—who are neither part of the regular army nor members of government or administration—for the purpose of carrying out warfare or espionage missions is not new and developed in historical times. The phenomenon of outsourcing for warfare, intelligence gathering, logistics, weapons development, security and consulting has been the norm throughout global military history and is becoming more widespread today. The Iraq War (2003) is one example, in which some 200,000 contract workers from private companies were deployed alongside 165,000 American soldiers.[3]

The phenomenon of outsourcing has also spread to the cyber field, especially as governments started using cyber for warfare and intelligence gathering. The two main reasons for outsourcing in intelligence gathering, cyber weapons development, and carrying out cyber operations are attributed to cutbacks in personnel and budgets and to quick technological developments in the field of information and communications technologies in the civilian

1 Andrea Mitchell and Ken Dilanian, "WikiLeaks Release already Damaging U.S. Intelligence Efforts," *NBC News*, March 10, 2017, https://nbcnews.to/2JTpPkR.

2 Eric Geller and Cory Bennet, "NSA Contractors Back in Spotlight after Reported Russian Theft," *Politico*, May 10, 2017, https://politi.co/2ERp7jI.

3 Alan Axelrod, *Mercenaries: A Guide to Private Armies and Private Military Companies* (Thousand Oaks, CA: CQ Press, 2014), pp. 3–8.

sector, which has provided the private market with a clear technological advantage over governments.

Outsourcing in both the fields of intelligence and offensive cyber capabilities occur on several levels. In many cases, research and development functions have been privatized in order to receive access to advanced technology and to quickly develop weapons. In other cases, cyber operations are being privatized because privatization provides governments with plausible deniability and the ability to absolve themselves of responsibility the moment the source of the attack is identified and thus avoid public relations damage or retaliation. It is important to distinguish between the outsourcing of cyber warfare and operations and the privatization in Western countries that includes support operations, such as research, development, and information gathering and processing.

In recent years, the theft of hacking tools, malware and spyware from the computers of intelligence agencies and cyber agencies' internal employees or contractors, along with discussions and statements about the role of the contractors, demonstrate the potential risk in privatizing support activities for operations. Examples from the physical world also indicate that the trend of privatization in the cyber field could spill over into other activities, such as carrying out offensive operations in cyberspace, even among Western governments.

The basic premise of this article is that there is a connection between the phenomenon of outsourcing and an increase in the proliferation of sophisticated cyber weapons. The article suggests ways to handle the risk and to minimize its consequences. Specifically, this article focuses on leaks over the past few years of hacking programs and cyber weapons, which could be the reason for the increase in the proliferation of these weapons, and examines whether these leaks can be connected to contractors. The article examines whether programs or codes have been stolen, sold without approval or leaked, and whether they could be used afterwards for attacks. In addition, this article looks at incidents of negligence in which there was the potential for the theft or leak of components that could be used for attacks. Leaks of cyber weapons, whether malicious or as a result of negligence, can create a situation in which states lacking resources or high level technological capabilities, terrorist organizations, or criminals—can repurpose malware and thus equip

themselves with advanced capabilities that they did not previously have.[4] Therefore, the proliferation of cyber weapons is defined here as the sale by unauthorized bodies, theft, or leak of hacking components, information on zero-day vulnerabilities, and malicious codes, which could potentially reach or already has fallen into the hands of others.

The article explains the phenomenon of outsourcing within the US intelligence and cyber community, as well as its advantages and disadvantages. The aim of the article is not to rule out outsourcing, as it turns out that also systems operated by permanent government employees are being hacked, enabling the theft or leak of cyber weapons or classified materials also from organizations that belong to the government. The article also seeks to increase awareness of the need for increased government supervision and for placing responsibility and accountability on government bodies or private companies that work for governments. Supervising, maintaining procedures, bestowing responsibility, and applying regulation, along with technological aids, can help government bodies supervise contract workers. Economic incentives can also help contractors improve their cyber security and encourage them to provide their employees with training on cyber hygiene and better supervise their work.

Outsourcing and Privatization of Intelligence and Cyber Services—A Theoretical Framework

This section suggests a theoretical framework for outsourcing the functions and activities that are reserved for cyber and intelligence agencies. It is important to note that outsourcing varies by country and is generally dependent on the historical context and organizational culture. However, outsourcing has a number of inherent advantages and disadvantages that should be discussed.

Why Do Governments Privatize Intelligence and Cyber Services?

Budget and personnel

Outsourcing is a practice that aims, first and foremost, to increase the efficiency of an organization and to save costs. The incentive to take activities outside of the organization and transfer them to external companies or workers is

4 Daniel Cohen and Aviv Rotbart, "The Proliferation of Weapons in Cyberspace," *Military and Strategic Affairs* 5, no. 1 (April 2013): 49.

based on the idea that organizations are unable to optimally perform all their activities; thus, in order to increase their competitive advantage, they must focus on their core activities and on those at which they excel and transfer all non-core activities to external companies.[5]

This theory of outsourcing is also relevant to the field of intelligence and cyber. Since intelligence agencies do not need to maintain a competitive advantage in the market, outsourcing serves mainly to reduce costs and streamline the organization. In terms of the development of cyber weapons, privatization has become a way of coping with budget cuts and personnel shortages in intelligence agencies. It should be noted that the problem of personnel shortages could result not only from budget cuts, but also from personnel restrictions and quotas that are imposed on intelligence agencies by supervisory bodies, and/or the departure of skilled personnel for the private market. Budget cuts in resources and/or personnel force intelligence agencies to employ fewer internal personnel, and as a result, they are unable to offer high salaries in order to attract talented and skilled personnel. This situation leads to the establishment of private companies that can offer better employment conditions, and thus recruit high-quality personnel.

An example of needing to cope with budget and personnel cuts can be seen at the end of the Cold War. The fall of the Soviet Bloc led to the dissolution of the main adversary of the United States, around which its massive intelligence apparatus had been built over several decades. As a result, the intelligence agencies faced extensive budget cuts and were forced to fire many employees and send others to early retirement. The cuts to the budgets and personnel of US intelligence agencies during the years 1990–1995 amounted to 16 percent of the budget and 20 percent of the personnel of the entire intelligence community. Among the intelligence agencies, the NSA suffered the most significant cutbacks: around a third of the agency's budget was cut during these years, leading to a similar cut in its labor force. Despite these changes, the US intelligence agencies quickly faced new challenges and a range of new global threats, including concerns about the security of nuclear weapons in the new post-Soviet states, along with drug trade, organized crime, terrorism, and ethno-political conflicts.

---

5 Ian McCarthy and Angela Anagnostou, "The Impact of Outsourcing on the Transaction Costs and the Boundaries of Manufacturing," *International Journal of Production Economics* 88 (2004): 62.

Surge capacity

Outsourcing is also an efficient practice for dealing with a possible discrepancy between the force structure of intelligence agencies—and later among cyber agencies within the defense apparatus—and the operational requirements relating to the number of targets or threats. Outsourcing enables flexibility and the ability to allocate skilled personnel and resources in order to cover a large number of threats simultaneously as needed.[6] Flexibility is necessary as a result of the development of the threat environment to national security and the appearance of different scenarios deviating from the focus on conflicts between countries, such as terrorism, the proliferation of weapons of mass destruction, international criminal organizations, genocide, ethnic conflicts, and, in more recent years, the cyber threat.[7] The need for flexibility also applies in the cyber age as new products on the market, such as operating systems, mobile phones, and apps, require focusing on the discovery and research of security vulnerabilities and the development of exploits.

Rapid pace of technological advancements

The rapid pace of change in communications and information technology is another factor that provides a significant advantage to the private market's analysis and processing capabilities. From the 1970s until the early 1990s, intelligence agencies believed that governments had the best access to R&D of advanced technologies and of information gathering and analysis systems. This belief eroded as information became cheaper and more readily available.[8]

The connection and the increasing access to the internet since the 1990s led to sharp and exponential growth in the number of users using networks for the purpose of interactions and exchanges of information, cooperation, and more. These changes apply not only to computers but also to all electronic devices that communicate with other devices, such as satellites, command and control systems, and so forth. The appearance of technologies, such as cell phones and satellite communication, advanced sensors, powerful processors, and encryption programs, provided the private market with a

6 Glenn James Voelz, *Managing the Private Spies: The Use of Commercial Augmentation for Intelligence Operations* (Joint Military Intelligence College, 2016), p. 2.

7 Bruce Berkowitz and Allan Goodman, *Best Truth: Intelligence in the Information Age* (New Haven and London: Yale University Press, 2010), pp. 51, 56.

8 Ibid, p. 23.

significant technological advantage over legacy systems that are sometimes still used by government, military, and intelligence bodies.

These changes also led to behavioral and cultural changes related to the handling of accessible and readily available information. In the past, information was a rare and valuable resource and considered the province of intelligence agencies; the information and technology revolution, however, made information and data more readily available. The competitive mechanisms of the private market, according to which technological companies develop new products and technologies and launch them at a fast pace, provides this market with an almost constant advantage.[9] In addition, the private market responds better to technological developments and changes, enabling quicker responses and the provision of superior services. This is even more so when it comes to exploiting information technologies. Under these conditions, the challenge of the intelligence agencies does not relate to whether they should turn to the private market to receive access to advanced technology, new services, and research and development but rather how they should exploit the advantages of the private market for security needs.

In the American case, we can point to technological developments in the field of information and communications technologies and the transitions in countries such as Libya, Iraq, Syria, Iran, and North Korea that have moved from using radio circuits to using communications infrastructure buried underground and optical fibers. These changes have posed a challenge to the SIGINT capabilities of US intelligence and have required it to constantly invest in technology.[10]

Difficulties in attributing cyberattacks

One of the well-known challenges of cyber warfare and one of its great advantages for the attackers is the difficulty in attributing cyberattacks. Unlike kinetic attacks, in cyberspace it is difficult to trace and identify the source of the attack. Even when the computer that carried out the attack is discovered, there can be no assurance as to whether it belongs to the assailant, or whether it has in itself been hacked and used for the purpose of the attack without the knowledge of its owner. In addition, hackers have many tools

9 Ibid, pp. 18–23.

10 Matthew Aid, *The Secret Sentry* (New York: Bloomsbury, 2010), pp. 196–198.

that enable them to cover or erase their tracks, to mislead investigators, and to destroy evidence.[11]

Transferring the execution of offensive cyber operations to private hands makes it even more difficult to attribute the attack, as even if the attacked party succeeds in tracing the assailants, it will have to prove that a government was behind the attack. Thus, transferring offensive cyber operations to private hands can provide governments with plausible deniability and minimize the chance of a response from the attacked state.

Exporting activities that do not comply with a country's laws or constitution
Exporting activities to develop hacking tools and executing offensive cyber operations can raise questions about the accountability and oversight when these activities are authorized and approved by the government but are conducted beyond the jurisdiction and supervision of formal supervision and review bodies, such as parliamentary committees and regulatory bodies. As third parties, private companies that carry out offensive cyber operations and espionage for intelligence agencies are not subject to the regulatory bodies nor to the supervision that could delay or prevent operations, which are seen as essential and whose secrecy and speed of execution are vital for achieving their objective. This aspect, which has both advantages and disadvantages, previously has been discussed in the context of interrogating terrorism suspects but becomes even more significant when related to the need to exploit breaches and vulnerabilities in order to hack into computers and networks as part of an active defense operation, counter-espionage, or to prevent terrorist attacks.

The Risks and Disadvantages of Outsourcing in Cyber and Intelligence Fields

The phenomenon of outsourcing in cyber and intelligence fields involves also risks and disadvantages. Some of these risks and disadvantages have been discussed in the contexts of outsourcing in the fields of physical warfare, interrogations, and assistance in targeted killing operations. Cyberspace, in particular, is a relatively new area of warfare, uniquely characterized by an extensive attack surface; a wide spectrum of attackers with different

11 Bruce Schneier, "Attack Attribution in Cyberspace," *Schneier on Security*, January 8, 2015, https://www.schneier.com/blog/archives/2015/01/attack_attribut.html.

backgrounds and interests, including civilians such as criminals or companies; an absence of physical distance and of physical borders; and a lack of clear definitions of what is legal and what is not. These characteristics of cyber, together with the risks and disadvantages of outsourcing in the fields of security, military, and warfare, render outsourcing risky for civilians, companies, government bodies, and organizations, which are far from the battlefield and are not involved in warfare. Another risk inherent in outsourcing is that operations dependent upon security clearance can be subjected to misuse and corruption.

Competition between the private market and intelligence agencies

Outsourcing has led to the creation of a private market for government activities. The growth of this market creates the effect of an infinite loop: The outsourcing of an increasing number of governmental functions leads to the growth of the private market and increases the salaries it offers. This places government organizations, including intelligence agencies, in competition with the private market, which attracts employees from these organizations and all talented workers available in the market.

The high salaries and better benefits offered by the private market also lead to the phenomenon of a "revolving door," known in the United States also as "bidding back," in which government employees leave for the private market and return to work for government agencies as private consultants at higher salaries. This phenomenon creates a flow of cyber and intelligence agency employees into the private market, thus causing a brain drain that exacerbates the government personnel problem, which they had tried to solve through outsourcing in the first place.[12]

In particular, the American private market grew sharply in the 2000s following the burst of the dot-com bubble,[13] which created a reservoir of personnel for defense agencies. Several companies, established by former members of the defense and intelligence agencies, hired the services of analysts

12 Patrick Radden Keefe, "Don't Privatize Our Spies," *New York Times*, June 25, 2007, https://www.nytimes.com/2007/06/25/opinion/25keefe.html.

13 The dot-com was an economic bubble that grew in 1997–2001, when many internet companies were established as businesses and customers alike adopted the internet, together with the fast growth of stock prices, speculation on their value, and the availability of investment money. With the bursting of the bubble, many internet companies became obsolete and closed.

and former military and intelligence personnel and created divisions and departments that initially engaged in intelligence and later in cyber activities. These companies were the only ones whose employees had both sufficient experience and security clearance. The major defense contractors, such as Boeing, Lockheed Martin, and Northrop Grumman, also created departments that deal with cyber and the development of hacking components.

Figures on the total extent of outsourcing in the fields of intelligence and cyber are classified information, which makes it difficult to properly study the scope of the phenomenon. However, figures from 2007 pointed out that around 70 percent of the US intelligence budget was allocated to private companies.[14] According to rough estimates given by a former CIA agent in an article written for *Time* magazine, contractors constitute around 50 to 60 percent of the CIA's workforce.[15] Today around 80 percent of the approximately 45,000 contract workers employed in the field of intelligence in the United States belong to five private corporations: Booz Allen Hamilton, CSRA, SAIC, CACI International, and Leidos. All five companies are located in Virginia and are also involved in the development of hacking tools and cyber warfare.[16]

Lack of supervision, monitoring, and control

In contrast to intelligence, espionage, and cyber agencies that are subjected to partial supervision by parliamentary committees and congressional bodies, actions of privatization, outsourcing, and the transfer of sensitive activities to private hands are done without government supervision and control while regulatory bodies do not have the ability to examine the degree of legality when they are carried out by private entities. Furthermore, private companies may feel less of an obligation to provide full and reliable information to regulatory and supervisory bodies. In addition, many countries have laws that direct security and intelligence agencies how to carry out tenders, sign

14 Simon Chesterman, "'We Can't Spy . . . If We Can't Buy!': The Privatization of Intelligence and the Limits of Outsourcing 'Inherently Governmental Function,'" *European Journal of International Law* 19, no. 5 (November 2008): 1056, https://doi.org/10.1093/ejil/chn055.

15 Robert Baer, "Just Who Does the CIA's Work?," *Time,* April 20, 2007, http://content.time.com/time/nation/article/0,8599,1613011,00.html.

16 Tim Shorrock, "Why does WikiLeaks keep Publishing U.S. State Secrets? Private Contractors," *Washington Post,* March 16, 2017, https://wapo.st/2WkVO3M.

contracts with private companies, and complete the purchase of products or services; in most cases, however, these laws do not include a clear and precise definition of processes for supervising the hiring of outsourced companies or monitoring their conduct or that of their employees. Contract workers in the cyber field still must meet minimum security clearance conditions, a process that in the United States is known as long and slow and is affected by arguments over budgets between the Department of Defense and the Office of Personnel Management. This has resulted in a lack of competition among the contractors themselves, including among US intelligence and cyber agencies. Although cyber agencies in the US defense forces need the ability to quickly hire new employees, the slow process of providing security clearance has led to a rising demand for former employees with security clearance, thus causing a lack of competition between the contractors.[17]

A tender issued by the NSA to develop the Trailblazer system for mining data from cellular and email communication manifests the absence of competition in the private market regarding the development of cyber and intelligence gathering tools. The tender was awarded to SAIC in 2002, for 280 million dollars. By 2005, however, the cost of the project had ballooned to over a billion dollars, and the project was later described as a total failure. Nonetheless, when the NSA announced the ExecuteLocus program, whose aim was to replace the Trailblazer system, the contract was again awarded to SAIC despite its previous performance.[18]

Another issue in terms of outsourcing relates to defining which functions are reserved only for government and defense agencies and which can be privatized.[19] The contract for translation services signed with the contractor CACI International is an example of this problem. The company provided interrogators to the military police, which was responsible for the interrogation of Iraqi prisoners during the invasion of Iraq in 2003. According to an investigation that began in 2008 following a lawsuit filed against CACI, the company's interrogators reportedly abused prisoners and violated human rights.[20] This incident provides an example for awarding an out-of-scope

17 Chesterman, " 'We Can't Spy…If We Can't Buy!,'" pp. 1068–1069.

18 Ibid., p. 1058.

19 Voelz, *Managing the Private Spies*, p. 23.

20 James Lesher, "Outsourcing Cyberwarfare: Drawing the Line for Inherently Governmental Functions in Cyberspace," *Journal of Contract Management* (Summer 2014): 7.

function to contractors which are not accountable and are not supervised. Another problem is the lack of supervision of the nature and scope of activities that can be privatized, which can lead contractors who are carrying out research, development, information gathering, and sometimes even internet operations to change the incentive for their activity out of commercial interests. These commercial interests, such as maximizing profits or extending contracts, along with conditions that are contrary to those of the free market—such as a lack of information and lack of competition—can harm their activities and results. For example, commercial interests can lead to biased conclusions or intelligence analyses in order to appease politicians or people within the intelligence agencies themselves. In the year before the invasion of Iraq, the Center for Counterterrorism Technology and Analysis, which was managed by the contractor SAIC, produced intelligence reports detailing the existence of Iraq's weapons of mass destruction and its intention to start a war. With the invasion of Iraq, SAIC was awarded contracts for intelligence and defense activities on Iraqi soil.[21]

Another possible result of the lack of supervision is mismanagement of information security. The threat of the proliferation of cyber weapons could significantly increase as long as employees who have access to source codes of programs or of development projects are not supervised. The absence of government supervision and control could enable the employment of people who do not see their work as a national mission, which could lead to negligence or the employment of people who have ideologies which may undermine the implementation of their tasks. Such situations could lead to leaks of classified information, attack and hacking components, and more. Although much has been said about cyber threats by other national actors, such as Russia, China, North Korea, and Iran, to critical infrastructure, economic sectors, companies and governments in the West, inadequate information security or hiring candidates who are not suitable for security positions, along with a lack of supervision and accountability, could lead to a situation in which cyber weapons developed by the best minds are leaked or stolen. This problem is exacerbated by the difficulty in monitoring and supervising malwares and exploits.

21 Donald Barlett and James Steele, "Washington's $8 Billion Shadow," *Vanity Fair* (March 2007), https://www.vanityfair.com/news/2007/03/spyagency200703.

These weapons could reach hostile parties and could be utilized against the very countries that had developed them in the first place, or against their allies. The leak of cyber weapons could enable countries with relatively low technical capabilities, terrorist or criminal organizations to carry out reverse engineering or to copy parts of code from sophisticated malware and reuse the stolen weapon.[22] For example, the Stuxnet worm, which was originally used to damage Iran's nuclear facilities, reportedly was copied and used for attacks on command and control systems in around fifteen power stations and chemical factories in Germany.[23]

Given these situations—in addition to the classification and compartmentalization practiced within cyber agencies—government bodies or organizations could be unaware of these problems, lacking the ability to impose policy or security standards on contractors, or could prefer the financial savings of hiring contractors. Examining the practice of outsourcing in the fields of intelligence and cyber reveals that, in addition to its advantages, it also has disadvantages (see Table 1 below), many of which surround the question of supervision and responsibility placed on contractors.

Table 1: Advantages and Disadvantages of Outsourcing in the Field of Intelligence and Cyber

Advantages	Disadvantages
Coping with budget cuts and personnel quotas	Competition between the private market and intelligence agencies
Surge capacity for coping with new and changing threats	Lack of competition between contractors
Access to advanced technology and rapid development	Lack of supervision over the types of processes and activities privatized
Increasing room for deniability (when using contractors for espionage operations or offensive cyber operations)	Potential for the politicization of processes and activities
Providing free rein—activity without legal constraints	Negligent or malicious management of information security and classified materials

22 Daniel Cohen and Aviv Rotbart, "The Proliferation of Weapons in Cyberspace," 50, 59.

23 Nicole Goebel, "Report says Stuxnet Computer Virus Hits German Firms," *Deutsche Welle*, October 2, 2010, https://bit.ly/2Z4fgPq.

Leaks of Cyber Weapons and Classified Materials: Case Studies from the American Intelligence Community

The Edward Snowden Affair

Background: The most infamous leak of classified material in recent years has been the Snowden affair. Edward Snowden was employed by the contractor Booz Allen Hamilton in 2013 and worked as an analyst for the NSA. In May 2013, about four months after he began his employment at Booz Allen, Snowden flew to Hong Kong, where, about a month later, he disclosed hundreds of thousands of classified NSA documents. These documents were published in the *Washington Post* and the *Guardian*, and afterwards by the *Der Spiegel* and the *New York Times*.

The connection between the incident and the proliferation of cyber weapons: Snowden's leaks disclosed the NSA's cellular communication and email correspondence surveillance techniques and capabilities. This included the disclosure of the PRISM program, which enabled the NSA to access Google and Yahoo data centers and extract information on civilians around the world, including American citizens.[24] Snowden's documents also disclosed databases of information gathered on civilians; information on analytical tools for gathering information from internet traffic; and information on the NSA's cooperation with communications companies and intelligence agencies of US allies.[25] Although most of the documents that Snowden leaked included information on the NSA's surveillance programs, it did not include the source codes of the components that were used for them. Nonetheless, the Snowden affair is a case that demonstrates the risk inherent when contractors are not supervised.

The motive: In several interviews given after leaking the documents, Snowden claimed that he did it out of a belief that the NSA's surveillance activity is illegal and violates the rights of American citizens. In addition,

24 Barton Gellman and Ashkan Soltani, "NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say," *Washington Post*, October 30, 2013, https://wapo.st/2WMEmoA.

25 Glenn Greenwald, "XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet,'" *Guardian*, July 31, 2013, https://bit.ly/2s5QlvF; Glenn Greenwald, "NSA Collecting Phone Records of Millions of Verizon Customers Daily," *Guardian*, June 6, 2013, https://bit.ly/2brf9H0; Scott Shane and Ravi Somaiya, "New Leak Indicates Britain and U.S. Tracked Diplomats," *New York Times*, June 16, 2013, https://nyti.ms/2YXifsS.

he accused the Obama administration of turning a blind eye to the espionage programs that began during the presidency of George W. Bush.[26] In this context, we can define Snowden's motives as ideological, which raises questions about the process of recruiting and placement of employees of contractors who are hired by US intelligence.

Harold Martin and the Shadow Brokers Leak

Background: Harold Martin was arrested in August 2016 on suspicion of taking home without any authorization around fifty terabytes of classified materials belonging to the NSA, CIA, and US Cyber Command. Martin had been employed for twenty years as a contract worker for seven different contractors who carried out projects for the Department of Defense, the CIA, and the NSA. In his last position, Martin had been a contract worker for Booz Allen Hamilton (for which Edward Snowden also worked). According to the indictment, Martin started stealing classified materials in 1996 and continued doing so until his arrest two decades later. Among the materials stolen were hacking components, documents describing techniques for hacking into foreign networks, and documents that detailed offensive cyber capabilities, processes and methods for gaining access to networks, and for protection of governmental systems and networks.[27]

The connection between the incident and the proliferation of cyber weapons: During the investigation, it was found that numerous materials that Martin had stolen were later found among the files leaked by the hacker group known as the Shadow Brokers.[28] These files were posted on the website Medium at the beginning of 2017 and included information on security breaches in systems and applications, along with details on methods of surveillance of computer systems, telephones, mobile devices, and websites.

---

26 Barton Gellman and Jerry Markon, "Edward Snowden Says Motive behind Leaks was to Expose 'Surveillance State,'" *Washington Post*, June 10, 2013, https://wapo.st/2JSMJbU.

27 Richard Chirgwin, "Ex-NSA Contractor Harold Martin Indicted: He Spent 'Up to 20 Years Stealing Top-Secret Files,'" *The Register*, February 8, 2017, https://bit.ly/2kuvq3f.

28 Scott Shane, Nicole Perlroth, and David Sanger, "Security Breach and Spilled Secrets Have Shaken the N.S.A. to its Core," *New York Times*, November 12, 2017, https://nyti.ms/2zznVzP.

The most prominent hacking component that allegedly had been stolen from Martin's computer was EternalBlue. EternalBlue is a code that exploits a vulnerability in the SMB (server message block) protocol, which is used for remote access of Windows operating systems. Since it was leaked, this component has been used for the spread of the WannaCry cyberattack, which affected over 230,000 computers in over 150 countries in May 2017.[29] EternalBlue continues to be commonly used around the world. According to a report by the Cyber Threat Alliance, an organization that shares intelligence on cyber threats, hackers continue to make use of this component in order to mine digital currency.[30] In this context, it should also be noted that the NotPetya global cyberattack was caused by using another NSA component called EternalRomance.[31]

Another example of a hacking tool that was leaked by the Shadow Brokers and may have been originally stolen by Martin is the DarkPulsar malware, which creates a backdoor and enables the installation of additional malware. In October 2018, Kaspersky Lab claimed that it had identified around fifty victims that were infected by DarkPulsar in nuclear energy, communications, IT, aerospace and research and development industries in Russia, Iran, and Egypt.[32]

The motive: At the time of this writing, the trial of Martin, whom his attorney has described as a compulsive hoarder, was still taking place and it had not yet been proven whether he sold the materials that he collected or whether they were stolen from his personal computer. Nonetheless, given that Martin took materials home over the course of years, it can be assumed that his conduct was negligent and improper vis-à-vis information security. In this context, many questions can be raised about the security measures of Booz Allen Hamilton, which did not discover Martin's actions even after

29 "EternalBlue – Everything there is to Know," *CheckPoint*, September 30, 2017, https://research.checkpoint.com/eternalblue-everything-know/.

30 "The Illicit Cryptocurrency Mining Threat," *Cyber Threat Alliance*, p. 14, https://www.cyberthreatalliance.org/wp-content/uploads/2018/09/CTA-Illicit-CryptoMining-Whitepaper.pdf.

31 Iain Thomson, "Everything you Need to Know about the Petya, er, NotPetya Nasty Trashing PCs Worldwide," *The Register*, June 28, 2017, https://bit.ly/2tjXLhX.

32 Catalin Cimpanu, "Kaspersky Says it Detected Infections with DarkPulsar, Alleged NSA Malware," *ZDNet*, October 19, 2018, https://zd.net/2OAL911.

it supposedly had increased its security measures and processes following Snowden's leaks.

The Vault 7 and Vault 8 Leaks from the CIA

Background: On March 7, 2017, WikiLeaks began posting a series of documents detailing CIA techniques, tools, and capabilities for carrying out electronic surveillance and cyber warfare. The series was called Vault 7, and the documents included were publicized in twenty-four parts between March and September 2017. In November of that year, the founders of WikiLeaks began leaking another collection of documents, which were called Vault 8.

In August 2017, Joshua Schulte was arrested as part of an FBI investigation into the distribution of pedophilic content. In a raid on his apartment, the investigators confiscated computers, mobile devices, and servers that contained pedophilic materials, as well as some classified material that he had taken from his workplace. Schulte worked as a software engineer for a CIA unit responsible for the development of codes for espionage programs and access operations. Schulte was not a contract worker, as initially had been estimated. During the investigation, it became clear that beginning in 2013, Schulte had uploaded a number of projects and codes that he wrote for the CIA to his public GitHub account, and had saved additional material on public servers for file-sharing.[33]

The connection between the incident and the proliferation of cyber weapons: the Vault 7 leaks throughout 2017, included hacking components for Linux and MacOS X operating systems for the purpose of espionage and information theft, as well as components used for intercepting communication, routing internet traffic, and shutting down security cameras.[34] The Vault 7 leaks mainly included documents describing hacking techniques and how to use hacking components. In contrast, the Vault 8 leak included source

33 Jason Koebler, "Alleged CIA Leaker has some of the Worst Opsec I've ever Seen," *Motherboard*, May 17, 2018, https://bit.ly/2IxR2ZP; John Walcott and Mark Hosenball, "CIA Contractors Likely Source of Latest WikiLeaks Release: U.S. Officials," *Reuters*, March 8, 2017, https://reut.rs/2QDdodm.

34 Pierluigi Paganini, "WikiLeaks – CIA Developed OutlawCountry Malware to Hack Linux Systems," *Security Affairs*, July 1, 2017, https://bit.ly/2uvnXTt; Sooraj Shah, "WikiLeaks Reveals CIA Tool Acting as SMS Proxy on Android," *Infosecurity-Magazine*, July 14, 2017, https://bit.ly/2vB7KfV; Swati Khandelwal, "3 New CIA-Developed Hacking Tools for MacOS & Linux Exposed," *Hacker News*, July 27, 2017, https://bit.ly/2BBfGRP.

codes and development records of the Hive project—a component that was used by the CIA to remotely control malware and receive information and data stolen from computers, whose existence had already been disclosed in the Vault 7 leak.[35]

The motive: The indictment against Schulte attributed his actions to malicious intent and an attempt to harm American national security. It claimed that Schulte gained unauthorized access to CIA computers from which the materials were stored, voluntarily transferred them to a third party, covered his tracks, blocked access by others to the system, and lied to his investigators.[36] Unlike Martin, Schulte denied these actions and claimed that he left the CIA as a result of an inability to continue to function, and as a result, the agency claimed that he was disgruntled and had turned him into a "scapegoat."[37] As of the time of this writing, it is not possible to know for certain what Schulte's motive was, but it is presumed that he had an active part in leaking the material which was publicized.

The Kaspersky Affair and the NSA Leak

Background: Nghia Hoang Pho worked as a developer for the TAO (Tailored Access Operations) division for developing hacking tools for the NSA from 2006 to 2015. Pho was accused of taking home classified digital materials and documents over the course of five years. His activity was discovered after Israeli hackers hacked into the computers of the Kaspersky Lab company and identified codes for NSA programs stored on them. The investigation showed that a Kaspersky anti-virus program that scans the computer and monitors malicious codes had been installed on Pho's computer. The anti-virus program had identified codes for NSA hacking programs that Pho took

35 Swati Khandelwal, "Vault 8: WikiLeaks Releases Source Code for Hive – CIA's Malware Control System," *Hacker News*, November 9, 2017, https://bit.ly/2zKk3dj.

36 "Joshua Adam Schulte Charged with the Unauthorized Disclosure of Classified Information and other Offenses Relating to the Theft of Classified Material from the Central Intelligence Agency," *Department of Justice*, June 18, 2018, https://bit.ly/2TuWMEU.

37 Matt Zapotosky, "Ex-CIA Employee Charged in Major Leak of Agency Hacking Tools," *Washington Post*, June 18, 2018, https://wapo.st/2HTjKTf.

home as malicious and had sent them to a cloud folder that the company uses for research purposes.[38]

The connection between the incident and the proliferation of cyber weapons: As mentioned, Pho had worked for the TAO unit, which develops codes for hacking tools. The codes that the Kaspersky software collected from his computer belonged to projects that he had worked on and were identified as malicious codes. The investigation showed that, contrary to the claims of Kaspersky Lab, the information from Pho's computer reached Russian intelligence officials. There are three main theories about how the information was transferred from the Kaspersky software to Russian intelligence. One theory is that Russian hackers exploited security vulnerabilities in the Kaspersky software. The other theory holds that Russian hackers intercepted the information while it was being transferred to the Kaspersky server in Moscow, and the third theory is that Kaspersky Lab worked for the Russian government, and from the moment the materials were discovered on Pho's computer, it actively stole them and transferred them to Russian government officials.[39]

The motive: Pho confessed and claimed in a letter submitted to the court that he suffered from social problems and that he had taken the materials home in order to go over them outside of work hours and to improve his performance at work as well as in the annual performance grade given to NSA employees.[40] Pho's case reveals negligence and deficient information security and neither malicious intent nor an ideological motive.

Ways of Addressing the Disadvantages of Outsourcing

Given the increasing scope of the phenomenon of outsourcing and its many advantages, outsourcing will likely continue to expand. Therefore, the focus should be on solutions for minimizing its negative impacts.

In order to address the problem of leaks of vulnerabilities and cyber weapons by both regular employees and contract workers who work for intelligence and cyber agencies of the defense apparatus, governments and

38 Nicole Perlroth and Scott Shane, "How Israel Caught Russian Hackers Scouring the World for U.S. Secrets," *New York Times*, October 10, 2017, https://nyti.ms/2g9jlRt.

39 Zack Whittaker, "What is Kaspersky's Role in NSA Data Theft? Here are Three likely Outcomes," *ZDNet*, October 9, 2017, https://zd.net/313DdIr.

40 Sean Gallagher, "NSA Employee who Brought Hacking Tools Home Sentenced to 66 Months in Prison," *Ars Technica*, September 26, 2018, https://bit.ly/2NHPOOk.

cyber security industries need to develop a defensive response. In addition, both the agencies responsible within the defense apparatus and the private contractor companies should be given more stringent supervision, with emphasis on the cyber security of systems and security procedures. Employees should undergo regular background checks, personal interviews, and their public records as well as their behavior on social media should all be checked. This information could shed light on employees' ideological or political views, which could affect their work performance. In addition, employees should also be required to undergo periodic medical and psychological tests, as these tests could help prevent any improper behavior.

Improving procedures and instituting recommended work practices for maintaining cyber hygiene can help to minimize negligence and unintentional leaks by employees. In order to improve the cyber hygiene of employees who develop or operate hacking tools and offensive cyber components, contract workers and employees of the defense and cyber agencies should be required to undergo periodic training and exams on identifying information security risks and cyber threats. In addition, procedures for working with classified information, including source codes and exploits, should be fine-tuned. Another possible solution for mitigating the theft of sensitive information, is a trend that has already begun in the United States and involves prohibiting defense and cyber agencies employees from using products of companies which hold connections to foreign governments, such as Kaspersky Lab's anti-virus products as well as communications equipment and devices of Chinese companies, such as Huawei and ZTE, which are obligated by Chinese law to cooperate with requests for assistance from China's intelligence agencies.[41] Security clearances should be made conditional upon abiding by these procedures and processes.

Minimizing negligence and information leaks can also be done with technological means. Technological solutions can help improve supervision of the cyber hygiene of employees or of contractors who work for them and include programs for scanning and monitoring external storage devices connected to the computers of cyber agencies or external companies, and scanning USB connections for any violations of information security and

41 Arjun Kharpal, "Huawei Says it Would Never Hand Data to China's Government. Experts Say it Wouldn't Have a Choice," *CNBC*, March 4, 2019, https://cnb.cx/2EMfgMr.

for copying materials. Tracking the movement of files on networks and monitoring the email accounts of employees could improve supervision capabilities and help maintain cyber hygiene.

In order to combat improper conduct specifically by contract employees, economic incentives can be included in contracts signed with contractors, thus encouraging them to track, monitor, and supervise their employees and their activity, and to engage in more meticulous and in-depth personnel recruitment processes. These incentives could be included as a condition for participating in future tenders or for ending contracts if not fulfilled.

Even after implementing these suggestions, however, it will be impossible to completely prevent leaks. According to the director of the National Counterintelligence and Security Center, William Evanina, the focus should be on how to identify leaks as quickly as possible and thus minimize their damage from the moment they are discovered.[42] Therefore, the bodies responsible for cyber within the intelligence and defense communities need to carry out risk assessments that include scenarios in which the source codes of cyber weapons are leaked and work to understand the extent of the damage and impact of potential leaks on future operations, along with their potential impact on cyber stability. Once programs that could be used for extensive global attacks have been leaked, the community of cyber agencies must be prepared to disclose quickly and discreetly the security vulnerabilities to the manufacturers.

Conclusion

A review of the case studies shows that while contract employees have been linked to cases of poor information security, negligence, deficient cyber hygiene, and have even expressed opinions or had ideological background that are incompatible with the security-oriented nature of their work, internal employees of the cyber agencies have also been responsible for the illegal proliferation of cyber weapons. Thus, negligence, lack of regulation, and the employment of people with a problematic background or who are incompatible with the nature of the work can be found both among contractors and among the internal employees of the intelligence and cyber agencies.

42 Patrick Tucker, "Can the NSA Stop the Next Snowden?" *The Atlantic*, September 18, 2016, https://bit.ly/2XliVru.

Outsourcing especially in the field of cyber has many advantages. Furthermore, the trend of outsourcing in this field is expected to expand and could even include carrying out offensive cyber operations. Nonetheless, the negative implications of outsourcing should not be overlooked, whether it is the leakage of offensive cyber capabilities and codes for hacking programs, or classified documents that disclose capabilities, methods, or operations. Even defensive actions carried out by private companies for government agencies, such as monitoring internet traffic and penetration testing, can be used for malicious purposes given a lack of supervision or negligence.

In order to address these problems, governments and cybersecurity industries must find a defensive solution that can handle the leaking of vulnerabilities, security breaches, and cyber weapons developed or used by contractors working for intelligence and defense agencies. This solution should include strict supervision of employees involved in developing and operating cyber weapons, including their undergoing periodic medical and psychological tests, comprehensive background checks, undergoing training and taking exams on the identification of cyber threats, and prohibiting the use of products manufactured by companies that have connections to foreign governments, especially strategic adversaries involved in cyber espionage. The use of technological aids can also minimize the negative impacts of the phenomenon.

Nonetheless, it seems that it will be impossible to completely prevent leaks of classified materials, including cyber weapons. Therefore, the cyber agency community must be prepared to identify leaks and cope with their potential damage the moment they are discovered.

The Academization of Intelligence: A Comparative Overview of Intelligence Studies in the West

Kobi Michael and Aaron Kornbluth

"Academization of intelligence" is defined as the academic research, conceptualization, and teaching about the world of intelligence. Its goal is to study the field of intelligence's essence, activities, and influence on the national security of the state and its decision-making processes. Policymakers and political leaders have recognized the increasingly significant role of intelligence in shaping policy and decision-making processes. These developments and concerns accelerated the academization of intelligence and gave the field its due attention and prominence. As the demand for intelligence practitioners increased, American and Western universities responded to the growing need for formulating academic programs and courses devoted to intelligence, which significantly accelerated the academization of intelligence. The United States, the United Kingdom, and Canada are at the forefront of efforts to academize intelligence. In other Western countries, such as Spain, France, and Germany, the process of academicization has been slower and burdened by the darker roles played by the intelligence services at certain points in history.

Keywords: Intelligence, academization of intelligence, academy, intelligence theory, intelligence journals, intelligence associations

Dr. Kobi Michael is a senior researcher at INSS. Aaron Kornbluth is an intern at INSS and a graduate student studying international relations at the Hebrew University in Jerusalem.

Cyber, Intelligence, and Security | Volume 3 | No. 1 | May 2019

Introduction

Although academic programs in intelligence already existed before the "Global War on Terror," the events of 9/11 and the US-led invasion of Iraq, which are perceived as intelligence failures, raised the subject of intelligence and security to the forefront of international relations. Policymakers and political leaders recognized the increasingly vital role of intelligence in shaping policy and decision-making processes and wondered whether the training of analysts in the intelligence community produced the intellectual flexibility and analytical rigor required to deal with the complex challenges and threats of the twenty-first century. These developments and concerns accelerated the "academization of intelligence" and gave the field its due attention and prominence. This development in the United States was emulated by university programs in Britain, Canada, Spain, and Israel, albeit in a more limited fashion.

Universities offered deeper research and methodological training as well as more critical, less-institutionalized, and less-conservative approaches. As the demand for intelligence practitioners increased, American universities responded to the growing need of formulating academic programs and courses devoted to intelligence that significantly accelerated the academization of intelligence. The increased attention on intelligence within the university framework greatly contributed to the field's emergence as an academic discipline in its own right and propelled scholarly research and writing on the topic.

The Academization of Intelligence—Definition

Academization of intelligence can be defined as the academic research, conceptualization, and teaching about the field of intelligence. Its goal is to study the world of intelligence's essence, activities, and influence on the national security of the state and its decision-making processes. The process of the academization of intelligence presupposes its interdisciplinary character and its inherent connection to cognate fields of knowledge, such as political science, international relations, history, psychology, and so forth. This academic activity is pursued through existing academic disciplines and paradigms, as well as through fundamental academic tools that include critical thinking, the development of theoretical infrastructure, and the writing and publishing of professional and scholarly literature.

Methodology and Research Questions

In this comparative study, the authors sought to survey the academicization process of intelligence in various Western states, including Israel, and describe its emergence as a field of serious academic instruction and research, better known as intelligence studies. In addition, we examined the field's academic characteristics, its long-standing debates, and the various approaches used in an attempt to understand the crux of intelligence studies, which possesses both the ability and responsibility of shaping contemporary and popular understandings of intelligence. The study focuses on three questions:

1. What led to the development of the academicization process of intelligence and its expansion in recent decades and how did it affect the nature of intelligence studies programs in various Western democracies?
2. Which aspects of intelligence do the various academic programs in the Western world emphasize, and is it possible to characterize different approaches to the field?
3. What are the different approaches used to study intelligence?

This article, resulting from a larger investigation conducted by the authors, is a qualitative study based on a review of existing intelligence literature (mostly professional journals), curricula of intelligence studies programs at various Western universities, and the websites of intelligence organizations and professional associations, all with an emphasis on the United States where the topic is the most developed. So that the study remains comprehensive, correspondence with researchers in the field from the United States and Canada was conducted as well as conversations with former practitioners from the intelligence community in Israel.

The Academicization Process

The Origins of Intelligence Studies

The study of intelligence as an academic subject has its roots in the United States, which is currently the dominant player in the field. Only a few years after World War II, Sherman Kent, an intelligence practitioner and academic, began discussing what he perceived as the natural and necessary integration between intelligence and academia—through the production of an intelligence literature—as an essential tool for the professional development of intelligence. The relevancy of Kent's work, "Strategic Intelligence for American World Policy," published in 1949, was not lost on intelligence and policy officials

as the United States assumed its important role in the post-war international order.[1] However, intelligence as a field of academic instruction and research was not prioritized nor prominent in the first decades after World War II. It regained public attention following a series of US intelligence scandals during the mid-1970s, which included attempted assassinations, invasive domestic surveillance, and abuse at the hands of American intelligence agencies. The 1975–1976 United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, better known as the Church Committee, led extensive investigations into the American intelligence community.[2]

In Britain, where its intelligence institutions were an open secret yet never officially acknowledged until the end of the Cold War, F. W. Winterbotham's 1974 book, *The Ultra Secret*, and other authoritative historical accounts of British intelligence's role during World War II, caused a surge in the popularity of intelligence in the United Kingdom.[3] Furthermore, the post-Cold War release of some records detailing the activities of British intelligence during World War II increased academic interest in historical archives research.

In Canada, the scandals that rocked the Royal Canadian Mounted Police in the late seventies and early eighties led to the publication of detailed annual reports by Canada's Security Intelligence Review Committee (SIRC) that was formed in conjunction with the Canadian Security Intelligence Service (CSIS). The relative transparency that was created through these incidents and investigations spurred academic interest in intelligence due to its relevancy to policy formation, especially in the conduct of international affairs during

1 See Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton: Princeton University Press 1949). Regarding his arguments for an intelligence literature, see Sherman Kent. "The Need for an Intelligence Literature," *Studies in Intelligence* 1, no. 1 (1955): 1–11.

2 Michael Goodman mentions Roberta Wohlstetter's *Pearl Harbor: Warning and Decision* (Stanford: Stanford University Press, 1962) as an influential book that piqued scholarly interest in intelligence matters in the United States. See Michael S. Goodman. "Studying and Teaching about Intelligence: The Approach in the United Kingdom," *Studies in Intelligence* 50, no. 2 (2006): 57–65.

3 See Goodman, *Studying and Teaching about Intelligence*. Goodman attributes this view to Wesley Wark who, in addition to Winterbotham's book, mentions the work by J.C. Masterman, *The Double-Cross System in the War of 1939–1945* (London: Yale University Press, 1972) as contributing to this turning point in UK intelligence awareness.

times of peace and war. Coincidental to this process was the retiring of many former American intelligence practitioners, many of whom took up teaching positions at universities and introduced intelligence-related courses.

The defining events of the twenty-first century (9/11, the invasion of Iraq in 2003, the London bombings in 2005, and so forth) prompted a dramatic increase in academic attention given to intelligence and the role it played and continues to play in government and modern society. Given this background, intelligence was defined as an important element of competent governance and decision making as well as "a tool for offensive war-making and defensive national security planning."[4] Accordingly, intelligence's place within the national security of the state became the natural focus of academic attention, in addition to topics surrounding other issues, such as the organizational structure of intelligence agencies and intelligence's vulnerability to politicization. Overstepping by intelligence organizations, such as in the United States, the Patriot Act, allegations concerning the use of torture, and the Snowden revelations prompted a flood of academic research on the proper boundaries of intelligence organizations in democratic societies, domestic surveillance, and abuse by Western intelligence agencies on both citizens and non-citizens alike, thus expanding the scope of the field and increasing intelligence's relevancy to the major issues of the twenty-first century.

Intelligence Studies: Developing an Academic Infrastructure

Before 1985, only a handful of intelligence associations and their publications existed in the United States, and they were geared mostly to current and former professionals in intelligence-related industries (mainly military). The events of 1985 (the arrests of Jonathan Pollard and John Anthony Walker, for example), known as the Year of the Spy, provided a strong catalyst that year for the establishment of a number of intelligence-related associations and journals around the world. These associations and journals supplied the necessary academic infrastructure and outlet for advancing knowledge in the field of intelligence studies and for increasing interest in the subject at all stages of academic learning.

The United States is home to several associations dedicated to this purpose of intelligence education and research, such as the Association of Former Intelligence Officers (AFIO) and the International Association

4 Ibid., 58.

for Intelligence Education (IAFIE). The AFIO, established in 1975, aims to raise awareness of the career needs of the US intelligence community among students at high schools and universities across the United States and publishes the *Guide to the Study of Intelligence*, which provides intelligence instructors with a literature review of significant works in order to assist with course development. The IAFIE, created in 2004, aims to bring government and academia together to advance the teaching of intelligence and serves as a catalyst for information sharing about intelligence training and education for both current and aspiring practitioners. The *International Journal of Intelligence and Counter-Intelligence* is a major US contribution to intelligence studies and includes internationally renowned intelligence scholars and former practitioners on its editorial board.

The United Kingdom and Canada house a number of influential associations and journals as well. The United Kingdom features its top intelligence scholars, such as Anthony Glees, Julian Richards, Peter Gill, Mark Phythian, Philip H.J. Davies, and Christopher Andrew in a variety of organizations dedicated to the historical study of intelligence. These include the British International Studies Association's Security and Intelligence Studies (SISG), the Oxford Intelligence Group, Brunel University's Center for Intelligence and Security Studies, and the University of Buckingham's Center for Security and Intelligence Studies. Additionally, the United Kingdom also publishes the well-known journal *Intelligence and National Security*, which produces numerous issues per year and accompanies its American counterpart as the leading scholarly publications on the subject. All these organizations and publications have had a slow but penetrating effect on British academia's approach to the subject of intelligence. In Canada, the Canadian Association for Security and Intelligence Studies (CASIS) is the country's premier association that promotes the study of intelligence. CASIS's goals are to foster the study of intelligence at universities and colleges as well as to provide a forum for academics and practitioners to discuss intelligence-related issues within the context of the constitutional values of society. In 2018, the *Journal of Intelligence, Conflict, and Warfare* was co-established by the Political Science department at Simon Fraser University and CASIS. The Canadian Carleton University also houses the Center for Security, Intelligence, and Defense Studies, which conducts policy-oriented research in the field and other crucial functions and activities.

France, Spain, and Germany also offer important contributions to the academic infrastructure of intelligence studies. France's Centre Français de Recherche sur le Renseignement [French Intelligence Research Center] (CF2R), established in 2000, aims to conduct academic research, publish works on intelligence and international security, and consult with stakeholders in government, business, and media on pertinent issues. At the same time, CF2R also seeks to raise awareness of intelligence as well as to demystify and explain its role and purpose to the French public. Spain's main intelligence-related output began in 2006 as *Inteligencia y Seguridad: Revista de Análisis y Prospectiva* but since 2016 has published exclusively in English under the title *The International Journal of Intelligence, Security, and Public Affairs*. Since 1993, Germany has housed the well-known International Intelligence History Association, which publishes the *Journal of Intelligence History*. The establishment of the Center for Intelligence and Security Studies (CISS) at Bundeswehr University in Munich (a federal research university associated with the German Armed Forces) in September 2017 is a major step up for the presence of intelligence studies in German universities. These initiatives are big leaps on the long road to changing Europe's overall cultural attitude toward intelligence studies and its inclusion in its universities' academic offerings.

Although the highly regarded status of intelligence in Israel should allow it to assume a central role in the numerous National Security Studies programs that populate Israeli universities, most of the discussions on intelligence are conducted primarily at research institutes and think tanks, which mainly organize seminars and conferences and publish policy-oriented periodicals and research papers. The most prominent and well-known research institute is the Institute of National Security Studies (INSS). INSS produces high-quality research in the field of intelligence studies through its tri-annual journal *Cyber, Intelligence, and Security* (replacing the institute's journal *Military and Strategic Affairs*), which focuses on the booming field of cybersecurity and intelligence. INSS also publishes the online publication *INSS Insight*, the quarterly journal *Strategic Assessment*, as well as various memoranda and books related to the field of intelligence. Other prominent Israeli research institutes that conduct research on intelligence and national security include the International Institute for Counter-Terrorism affiliated with IDC Herzliya, the National Security Studies Center at the University

of Haifa, the Begin-Sadat Center for Strategic Studies, and the Jerusalem Center for Public Affairs.

The Israel Intelligence Heritage & Commemoration Center (IICC) plays a key role in the promotion of intelligence education, research, history, and commemoration of fallen Israeli intelligence operators. The IICC runs two research institutes: The Meir Amit Intelligence and Terrorism Information Center (ITIC) and the Institute for the Study of Intelligence and Policy Research (ISIPR). The ITIC conducts research and analysis on Middle Eastern affairs, with an emphasis on anti-Semitism, the Palestinian issue, and developments in terrorist-sponsoring countries, namely Syria and Iran. The ITIC also publishes two periodicals: "News of Terrorism and the Israeli-Palestinian Conflict," and "Spotlight on Iran," which reflect the views of the Israeli intelligence community and are distributed to various academic and governmental institutions.

The latter research institution, the ISIPR, is regarded as the more objective of the two and aims to focus on intelligence as a profession (echoing the calls of well-known intelligence scholar Stephen Marrin). In an effort to promote this vision and foster scholarly discussion, the ISIPR also produces a new, bi-annual, and high-quality journal focusing on intelligence methodology entitled *Intelligence in Theory and Practice*. The journal is published both in Hebrew and in English. In addition to its journal, the IICC also publishes in-depth research papers on intelligence topics. Clearly, Israeli intelligence studies already possess a strong academic infrastructure that could support the field's increased participation in university programs.

Approaches to Intelligence Studies

There are a multitude of approaches to the study of intelligence, affected mostly by "the way intelligence is defined [as it] necessarily conditions approaches to research and writing about the subject."[5] This definition has been determined in different ways, often corresponding to a country's tradition of intelligence, culture of secrecy, and ethos of governance. For example, the American definition of intelligence generally revolves around the process of creating intelligence products from both secret and open sources for use by decision makers, whereas the British definition falls squarely in the realm

5 Len Scott and Peter Jackson, "The Study of Intelligence in Theory and Practice," *Intelligence and National Security* 19, no. 2 (2004): 141.

of secret information that is obtained by furtive means. These divergent definitions have a significant impact on the emphases of intelligence programs in the two countries and the approaches utilized in its study.

Additionally, the approach taken to study the multi-dimensional subject depends largely on the academic department in which intelligence studies is nestled. An intelligence program within a history department will approach intelligence differently than an intelligence program that studies it from a political science lens. The interdisciplinary nature of intelligence allows it to behave this way and for the different schools of intelligence to emphasize one approach over another.

The various approaches to intelligence are influenced not only by the fundamental differences between academic approaches and the understanding of what intelligence is but perhaps also by the differing relationships between the countries' intelligence and academic communities. In the United States, although academic prejudice against the intelligence community's entrance and participation in the academic discourse still exists,[6] it is possible to identify a more open and porous relationship between academia and US intelligence agencies relative to other Western democracies. A well-oiled "revolving door" —frequent transitions between academic and governmental spaces— helps to maintain a consistent presence of former intelligence professionals who can offer practical and experienced insight. Additionally, the historical development of intelligence studies in the United States as a social science came as a result of public senate inquiries into the functions, operations, and politicization of intelligence. Thus, this relatively open culture enables the dominant approach to US intelligence studies to include the construction of abstract theoretical models that provide an academic basis for the subject as well as to impart students with the professional skills of intelligence analysis in order to develop qualified entry-level candidates. This process is actively encouraged by US intelligence agencies, who hope to increase public interest and awareness of the nature and activities of intelligence and, through this, enhance the intelligence community's legitimacy and build a pool of potential recruits.

---

6 For a discussion of academic resistance to intelligence studies in US universities, see Matthew D. Crosston, "Fragile Friendships: Partnerships Between the Academy and Intelligence," *International Journal of Intelligence and CounterIntelligence* 31, no. 1 (2018): 139–158.

In Britain, this relationship is much more limited. The "British School" of intelligence studies is grounded mainly in historical case study-research, including specific decisions made by policymakers and how intelligence has influenced these decisions. This is due in part to the distance maintained between the public and the intelligence services. The Official Secrets Act 1989 deters current and former intelligence officials from speaking about their work and no deep inquiries into the intelligence services were conducted until the aftermath of the 2003 war in Iraq; only after 1979 did historians have access to the historical archives and the sanctioned official histories of the British intelligence services during the Second World War (other methods used in parallel was to research the "adjacent files" of the Foreign Office and the Home Office, as well as the archives of intelligence allies).[7] Additionally, the belief that universities should focus strictly on subject matter knowledge correlates with the opinion that training analysts is best left to the secret services, which is also influenced by this distance maintained between government and academia.

The different approaches employed by the American and British academic communities reflect not only the challenges facing the study of intelligence but also the richness and variety of the subject. This is heavily dependent on the nature of each country's relationship between intelligence agencies and academia as well as the traditions and culture of security. Essentially, the study of intelligence can either be predominantly historical and case study-based or it can be primarily abstract, theoretical, and social science-based. The American approach is more influenced by the social sciences, whereas the British approach is essentially historiosophic. In contrast to the British approach, which emphasizes historical case studies and relies on archival documents, the American approach emphasizes theorization and has a clear preference for the technical and procedural aspects of intelligence. Due to the historical and conceptual differences between the United States and the United Kingdom, the two countries diverge in their approaches used in teaching and research. This can be described as an American-Anglo continuum.

Stafford Thomas, an early American scholar of intelligence, detailed four oft-cited paradigmatic approaches to the study of intelligence: The *historical approach* uses case studies and famous personalities and is either memoir-based

7 See Len Scott, "Sources and Methods in the Study of Intelligence: A British View," *Intelligence and National Security* 22, no. 2 (2007): 185–205.

or archive-based; the *functional approach* focuses on operational activities and processes and delves deeper into more abstract issues; the *structural approach* examines the role of intelligence and security agencies in the conduct of international affairs; the final method is the *political approach,* which addresses policymaking and governance issues and concentrates exclusively on the political dimension of intelligence, including decision making, policy formulation, and so forth.[8]

In a later paper, Wesley Wark, a Canadian intelligence scholar, identified eight different projects/methodologies used in the approach to studying intelligence: *The research project* utilizes primary source archival evidence; *the historical project* produces case study-based accounts; *the definitional project* is concerned with defining the subject; *the methodological project* applies social science concepts to intelligence; that is, using case studies to test the theoretical deliberations; *the memoirs project* is designed to offer first-hand perspectives; *the civil liberties project* is inherently not objective and is designed to reveal the surreptitious activities of intelligence agencies where they impinge on domestic life; *the investigative journalism project* typically covers topics for which there are no historical archives available; and finally, *the popular culture project*—perhaps the latest avenue of research—considers relatively obtuse topics such as the politics of James Bond.[9] These projects can be used to identify four main areas of contemporary work: research/historical, definitional/methodological, organizational/functional, and governance/policy, which are reflective of the above-mentioned four paradigmatic approaches.

Finally, Len Scott and Peter Jackson reflect on three distinct approaches[10] that scholars use in order to achieve specific objectives. The first approach, preferred by historians in particular, conceives of the study of intelligence primarily as a means of acquiring new information in order to explain specific decisions made by policy makers in both peace and war. In this approach, attention is paid to the intelligence gathering process, the nature of the intelligence source, and the organizational structure of intelligence

8 Goodman, *Studying and Teaching about Intelligence.* See also, Stafford. T. Thomas, "Assessing Current Intelligence Studies," *International Journal of Intelligence and Counterintelligence* 2, no. 2 (1988): 217–244.

9 Wesley K. Wark, "Introduction: The Study of Espionage: Past Present, Future?" *Intelligence and National Security* 8, no. 3 (1993): 1–13.

10 See Scott, *The Study of Intelligence in Theory and Practice*.

organizations as intelligence travels up the decision chain. The second approach endeavors to construct general models that can explain intelligence success and failure. This is a more political science-based approach and focuses entirely on intelligence analysis and decision making. The aim is to identify and analyze the personal, political, and institutional biases that characterize intelligence organizations. The third approach focuses on the political function of intelligence and how it is used as a means of state control. Central to this approach are ethical issues arising from the activities of intelligence organizations and state power.

The State of Intelligence Studies

United States

Although the events of 9/11 raised the value of intelligence and placed it at the forefront, intelligence studies in the United States was slow to take off. The primary reasons were the dearth of qualified instructors, a lack of means to assess instructors' credentials, and the logistics of curriculum building and program creation. Although smaller initiatives, such as the CIA's Officers-in-Residence program, were already in place, only by 2005 did US academia experience a heightened capacity for intelligence studies. In the same year, the US government, through the Defense Intelligence Agency (DIA), initiated the US Intelligence Community's Center of Academic Excellence program (IC-CAE), which provided government funding to host universities and was intended to meet the longer-term human resource needs of the intelligence services. This program had a profound effect on the cultivation of intelligence studies as a serious academic discipline.

Internationally, the United States has the largest audience for intelligence studies and has the greatest number of undergraduate and post-graduate courses in the field. The above-mentioned initiatives provided funding and fed the nascent field of intelligence studies, allowing it to grow as a serious form of academic study, mostly by building on existing institutional capabilities across related disciplines. That being said, contemporary intelligence studies in the United States developed mainly within the fields of political science, history, and international relations.

Research examining the curriculum in US universities concluded that, as a general framework, there are three pillars to American degree-granting intelligence programs: the procedural pillar, the core pillar, and the domain

pillar.[11] The procedural pillar focuses on the performance of intelligence tasks and the acquisition of analytical skills. The core pillar addresses the organizational, historical, and ethical content areas of intelligence and offers an intellectual and theoretical framework for understanding the central issues surrounding intelligence. Finally, the domain pillar provides knowledge about the different types of intelligence, such as national security, criminal intelligence, cyber intelligence, and competitive intelligence. National security, with a heavy focus on terrorism, is most dominant in American universities, while the least developed is the business-related competitive intelligence.

From the survey conducted it could be concluded that universities are "training" students in intelligence rather than "educating" them about intelligence. Many universities strive to adopt this "training" methodology because they claim that US agencies look for this skill set in potential candidates. A look at Mercyhurst University's undergraduate intelligence studies degree reveals this emphasis in its core courses, which impart students with functional skills. These courses include "Intelligence Methods and Analysis," "Professional Communications," "Intelligence Writing and Presentation," and "Communicating Intelligence Analysis." The degree mission statement further emphasizes this point in that it seeks to "to provide its graduates with an advanced level of analytical skills . . . and the necessary background for students to pursue careers as research and/or intelligence analysts in government agencies and private enterprise."[12]

Intelligence scholars, such as Nicholas Dujmovic and Mark Lowenthal, highlight the opportunity cost of studying intelligence with the goal of employment in an intelligence organization; studying the subject as a major in US universities would take the place of subjects that are crucial to intelligence analysis, like foreign languages and computer science. These schools train students as "generalists"—those trained in the methods and mechanics of intelligence analysis—in lieu of "specialists" with expertise in specific subject matter. It is precisely on this issue that scholars diverge

11 See Stephen Coulthart and Matthew Crosston, "Terra Incognita: Mapping American Intelligence Education Curriculum," *Journal of Strategic Security* 8, no. 3 (2015): 46–68.

12 Mercyhurst University, "Intelligence Studies, Ridge College of Intelligence Studies and Applied Sciences," *Mercyhurst University*, accessed November 11, 2018, https://www.mercyhurst.edu/ridge-college-intelligence-studies-and-applied-sciences/intelligence-studies.

on what the division of labor should be between university education and intelligence agency training. The US university learning structure offers a simple solution: major in a specialized subject matter and minor in intelligence studies.[13]

Britain

As previously stated, the way a country defines intelligence, its historical background, and the structure and makeup of a country's intelligence community all contribute to different foci when considering the study of intelligence. These factors have immense importance in the way that intelligence is manifested in the academic world. In the United Kingdom, intelligence is defined as "information acquired against the wishes and generally without the knowledge of the originators or possessors. Sources are kept secret from readers as are the techniques used to acquire the information."[14] This opposes the US definition, which is generally held to be any information, from covert and overt sources, that is turned into an end-product for the consumption of decision makers. The difference in perspective across the Atlantic could be described as intelligence as "secret information" versus intelligence as a "process."

Anthony Glees has pointed out that this focus reveals a paradox between the American and British intelligence studies programs: The narrow definition of intelligence in the United Kingdom has led to a broader study of the subject (history), whereas in the United States, the opposite holds true (analysis). Glees suggests that one reason for this may be that the British intelligence community "believes that whilst it might be useful to them if some of their intelligence officers had degrees in intelligence studies, there is no particular reason why they should."[15] In the United Kingdom, there is much more emphasis on "education" rather than "training." This is partly because many UK universities are hesitant about the idea that universities should "train" their students.

---

13 See Nicholas Dujmovic, "Colleges Must be Intelligent About Intelligence Studies," *Washington Post*, December 30, 2016. See also Alessandro Scheffler Corvaja, Brigita Jeraj, and Uwe M. Borghoff, "The Rise of Intelligence Studies: A Model for Germany?" *Connections: The Quarterly Journal* 15, no. 1 (2016): 79–106.

14 Anthony Glees, "Intelligence Studies, Universities, and Security," *British Journal of Educational Studies* 63, no. 3 (2015): 282.

15 Ibid., 288.

Although there was already some scholarly work on the history of intelligence issues (the first revelations about British intelligence successes in World War II had appeared in the 1970s) and growing concern in the American and British public about intelligence failures and scandals, the British intelligence community remained resolutely secret. Nevertheless, 9/11 and the intelligence failures in the war in Iraq spurred a change in the British awareness of the intelligence community. The release of Lord Butler's *Review of Intelligence on Weapons of Mass Destruction* and other archived material caught the attention of academics, especially historians. The academic study of intelligence in the United Kingdom has developed overwhelmingly within the discipline of international history and focuses on mostly archive-based research. This is partly due to the distance maintained between academics and practitioners. This approach is reflected in the leading British journal on the topic, *Intelligence and National Security,* as it is geared largely toward historians.

Further evidence of the "British School" of intelligence studies can be compiled by cataloging the programs in intelligence offered in the British university system. Generally, courses on intelligence are found at the graduate level. Individual courses on the subject exist (mostly within history departments), and only recently have degree-granting programs in intelligence studies been established at the undergraduate level. These courses and programs in intelligence are usually combined with relevant topics in the field of intelligence as it applies to national security in the twenty-first century and focuses on the interaction between intelligence and war, politics, and international relations. In contrast with the US programs, the curricular content does not include instruction on intelligence analysis. The undergraduate programs of Strategy, Intelligence, and Security at Aberystwyth University and Security, Intelligence, and Cyber at the University are apt examples of this description.

At the master's level, intelligence programs are simply variations of international relations programs, aiming to produce scholars of the subject, not practitioners. Additionally, the focus on intelligence mostly is done through historical case studies, supporting the fact that the subject in the United Kingdom developed primarily from the study of history and less so from the theoretical and abstract social sciences. As an example of the above, the master's program in Intelligence and International Security Studies at

the King's College Department of War Studies informs prospective students that they "will develop an awareness of the ways in which intelligence issues manifest themselves in security issues in peace and war," and they "will also gain an understanding of ethical dilemmas associated with intelligence activity."[16] Included is one core course in intelligence, entitled "Intelligence in Peace and War." Not one course on the program's elective course list imparts a skillset to students. Rather, it is mostly subject-area focused akin to an international relations program. Brunel University's master's program in "Intelligence and Security Studies" is the one exception to the rule and includes one required course on "Analytical Methodology."

Canada

Initially, most of the official government publications relating to Canadian intelligence consisted largely of the various scandals that rocked the Royal Canadian Mounted Police (RCMP) during the late 1970s to early 1980s. However, since the creation of the Canadian Security Intelligence Service, upon recommendation by the McDonald Commission (a commission set up to investigate the RCMP whose job at that time was both policing and security intelligence), information on Canadian intelligence began to be publicized more steadily, principally by the Security Intelligence Review Committee. Since 1984, this body has been issuing detailed annual reports that provide insight into the realm of the CSIS as well as the general field of Canadian intelligence.

The field of Canadian intelligence studies is small but healthy. Most of the writing on intelligence in Canada has been done by Canadian academics; few non-Canadians have focused on the country. Those who write about security and intelligence in Canada are mainly historians by training, with some political scientists in the mix. Many of these scholars belong to Canada's premier intelligence research center, CASIS, which has held annual conferences and has encouraged the mingling of academics with practitioners since 1985 (established one year after the creation of CSIS and SIRC). Two motivations seem to dominate Canadian participation in intelligence studies: interest and duty. The second motivation is characterized

16 King's College London, "Intelligence and International Security MA," *King's College London*, accessed June 22, 2018, https://www.kcl.ac.uk/study/postgraduate/taught-courses/intelligence-and-international-security-ma.aspx.

by some academics who feel that they are performing a public service by writing about an area that is normally hidden from public view and where the exercise of democratic controls is necessary.

Canada's universities that supply intelligence-related courses and programs are mainly on the master's level and, for the most part, utilize a historical approach. The focus is interdisciplinary and less on professional skills; it is assumed that students already have acquired critical thinking, written and oral communication skills, and analytic skills at the undergraduate level. Intelligence-related programs include Carleton University's Center for Security, Intelligence, and Defense Studies at the Norman Patterson School of International Affairs; Simon Fraser University's Terrorism, Risk, and Security Studies Program; University of Ottawa's summer course on Intelligence and Security; and the Center for Conflict Studies at the University of New Brunswick, which publishes the *Journal of Conflict Studies*.

Several historical periods draw the steady attention of researchers, including World War II, the Cold War, the events surrounding the Quebec Liberation Front (FLQ), the 1981 McDonald Commission, and the creation of CSIS. In addition, several major themes have dominated the Canadian security and intelligence literature since its inception. Especially due to the RCMP scandals, questions of the proper limits of the law and ethics have been at the core of the literature. Another theme is whether Canada should have a separate civilian intelligence service and the difficulties that it faces as well as the nature of its review and oversight by SIRC. More attention is paid to the oversight and review mechanisms than the effectiveness and practices of the Canadian intelligence community. Finally, another recent interest is the question of whether Canada should even have a foreign intelligence service.[17]

Germany

Wolfgang Krieger, a prominent German intelligence historian, wrote in 2004 that "German historians have so far shown little interest in the history of intelligence services and in the role the craft of intelligence played in national and international politics."[18] The state of German intelligence studies

17 See Geoffrey R. Weller, "Assessing Canadian intelligence Literature: 1980–2000," *International Journal of Intelligence and Counterintelligence* 14, no. 1 (2001): 49–61.

18 Wolfgang Krieger, "German Intelligence History: A Field in Search of Scholars," *Intelligence and National Security* 19, no. 2 (2004): 185.

is weak relative to the United States and the United Kingdom, as there is not even one dedicated program in the field offered in the country. A number of factors contribute to its underdevelopment: a lack of declassified documents, the complete absence of former intelligence officials at universities (no "revolving door"), and the mindset of German academia, which is not fond of research on defense and security issues as a result of Germany's Nazi and Gestapo experiences during World War II, as well as the experiences of the Cold War.[19]

However, there has been gradual change. At the end of the Cold War, Stasi archives suddenly became available along with some Russian records as well. In response a small group of German historians interested in the subject formed a study group to capitalize on this new opportunity for research. They established themselves as the International Intelligence History Association and, in 2001, started the *Journal of Intelligence History*, co-edited by Chris Moran of the University of Warwick and Shlomo Shapiro of Bar-Ilan University. The CISS plans in 2019 to begin a master's degree program in Intelligence and Security Studies at the Departmental Branch of the Intelligence Services of the Federal University of Applied Administrative Sciences (Hochschule des Bundes) and at the Bundeswehr University Munich. The program will focus on issues related to intelligence and security and professional skills, akin to the American School. The master's program will be available only to members of the German intelligence services.[20] Despite these developments, the obstacles facing German intelligence studies remain.

Spain

Since 2005, intelligence studies in Spanish academia has been increasingly supported by the Spanish Ministry of Defense and by the Centro Nacional de Inteligencia (CNI), the Spanish intelligence service that was established in 2002. The increase of Spanish academia's engagement with intelligence studies has come in response to its intelligence community's desire to correct inaccurate public perception of intelligence and to publicly promote a "culture of intelligence" through universities, also known as the CNI's Intelligence

19 Ibid. See also Corvaja, *The Rise of Intelligence Studies*.

20 See Universität der Bundeswehr München, "Center for Intelligence and Security Studies," *Universität der Bundeswehr München,* accessed November 20, 2018, https://www.unibw.de/ciss.

Culture Initiative. At the heart of this intelligence culture initiative is the CNI's development and management of its relationships with academia in order to benefit from the latter's expertise and thorough research in pertinent areas. As a result, the normalization of intelligence studies as an academic discipline in Spain has been one important outcome.

Although much has been accomplished, a number of obstacles still prevent intelligence studies in Spain from further maturation, such as a dearth of experienced faculty, a lacuna in specialized literature in foreign languages, the absence of a clear conceptual and theoretical definition of intelligence, as well as a lack of a common understanding of the word intelligence in Spain outside of its intelligence community (no culture of intelligence); increased business value in the use of the word "intelligence" even when there is no connection to the Spanish intelligence community; the slow and laborious process of declassification; and the preoccupation with intelligence conspiracy theories and legends.[21] Ultimately, "the development of Intelligence Studies in Spain will depend on the successful creation of an academic culture that understands that the study of intelligence in a democratic society is not only normal, but fundamental, and that the Intelligence Community is part of the machinery of the modern state."[22]

France

In France, there is an attitude among the public and academia that resembles Germany's relationship with intelligence studies, in that there are historic and cultural reasons for the apparent disregard for the subject. First, intelligence work has never been held in high regard by politicians, the military, academics, or economists, and "espionage" has been looked upon negatively since the Dreyfus Affair. Second, historians and political scientists traditionally had not considered intelligence to be an important parameter of statecraft, nor did they consider the intelligence services as significant stakeholders in state policy. Third, the secret nature of intelligence work did not facilitate the work of researchers, and the issue of access to documents for a long time stymied historical research.

---

21 Gustavo Diaz Matey, "The Development of Intelligence Studies in Spain," *International Journal of Intelligence and Counterintelligence* 23, no. 4 (2010): 748–765.

22 Ibid., 760.

The emergence of intelligence studies in the world of French academia is principally a result of the information revolution and ever-increasing global competition during the early 1990s. Economic stakeholders began to take a great interest in integrating intelligence into businesses. In response to this new market demand, universities specializing in business, management, and economics began to provide courses or other specialized post-graduate courses on "business-intelligence." In parallel, research and publications on the subject expanded. In addition to the comparative advantage intelligence can offer to businesses, the attacks of September 11 thrust intelligence into the spotlight as an essential instrument in domestic security, military defense, and foreign policy. However, French ideas of intelligence have mostly focused on domestic matters and internal security in defense of national interest.[23]

Israel

Security is central to the Israeli experience and intelligence studies are extremely relevant within the Israeli context. Public awareness of security issues and the unique characteristics of socio-military relations in Israel contribute to a porous relationship between the intelligence and security communities and Israeli academia. This is an advantageous condition for the growth of intelligence studies. Israeli academia is aflush with the presence of retired security and intelligence establishment personnel, or at least those who served for several years in military intelligence units during their mandatory military service. Additionally, they have accumulated rich and valuable professional experiences as well as broad networks of current and former security and intelligence officials. Research in the field of intelligence in Israel and its low barrier to entry for the general public is unique and remarkable.

Many scholars involved in intelligence-related research at universities are situated in political science departments. Nevertheless, their research methodologies are mainly historical (similar to the "British School") and focus on Israeli intelligence history, especially in regard to intelligence failure (since intelligence successes is rarely publicized). Other research topics include comparisons between the Israeli and foreign intelligence communities, international and methodological aspects of intelligence,

23 Eric Denécé and Gérald Arboit, "Intelligence Studies in France," *International Journal of Intelligence and CounterIntelligence* 23, no. 4 (2010): 725–747.

the relations between Israeli security services and the rule of law, and the organizational structure of the Israeli intelligence community. One common obstacle to Israeli scholarship in intelligence studies is Israel's strict policy regarding the declassification and publication of past intelligence-related records.

The teaching of intelligence at Israeli universities is mainly found in only a handful of courses that are part of MA-level programs in National Security and International Relations. Programs in the field of national security for students who are not part of the security establishment are few. The oldest program for civilian students in security studies is Tel Aviv University's interdisciplinary MA program in Security Studies, situated in the Political Science Department. Another program is the BA in Government with a specialization in homeland security and counterterrorism at the Interdisciplinary Center in Herzliya. There was one notable attempt in 2015 by world-renowned Professor Shlomo Shapiro and Dr. Ephraim Lapid to establish an MA-level intelligence studies program in Bar-Ilan University's Political Science Department; this program, however, no longer exists.

Intelligence Communities and the Academicization of Intelligence

The approach of intelligence agencies to the academization of intelligence depends heavily on the general and national way of life, as well as the political values, and the culture of both intelligence and of higher education. Defining "intelligence" is also an important determining factor in the approach to outside scrutiny. The difference in attitudes reflects not only on the academic relationship between the intelligence communities and academia but also on the developmental path of intelligence studies in their respective countries.

US intelligence agencies are embracing the growing interest in intelligence studies and promoting and encouraging research and teaching in this field through initiatives such as geospatial intelligence scholarships and certificates, the Intelligence Community Centers of Academic Excellence (IC-CAE), and the Officers-in-Residence program. Within the American intelligence community itself, the inclusion of an academic component to their internal training paradigm is fixated on acquiring procedural knowledge and a common analytic vocabulary. This is manifested by numerous analytic training classes

at CIA University (the CIA's training apparatus), which incorporate and emphasize certifiable Structured Analytic Techniques (SATs).[24]

In the United Kingdom, secrecy and separation characterize the academic-intelligence relationship. Although undeniably attracted to one another, the British government has maintained the separation of intelligence services and the academic study of intelligence through various means, such as the exclusion of intelligence agencies from the British Freedom of Information Act. All this makes access to archival materials tightly controlled and restricted, even though the end of the Cold War led to a gradual loosening of the government's approach to archival release. British intelligence agencies generally do not engage directly with academic intelligence programs except in more technical fields, such as cybersecurity. There has been some degree of openness in recent years pertaining to agency-academic engagement, but the trend is not widespread and remains picky and exclusionary.[25] The establishment of a closed ten-week professional development program at King's College of London's Department of War Studies following Lord Butler's 2004 report on UK intelligence exemplifies the inclusion of academic content in British intelligence's training of analysts.[26]

In Canada, when Carleton University's Canadian Center for Intelligence and Security Studies (CCISS) was founded, it held workshops for intelligence practitioners. Academic research papers of interest to intelligence were also encouraged and were printed and distributed under the Canadian intelligence budget. Currently, at most, PhD students may be encouraged to research an area of particular interest to intelligence agencies and given some access to

24 John A. Gentry, "The 'Professionalization' of Intelligence Analysis: A Skeptical Perspective," *International Journal of Intelligence and CounterIntelligence* 29, no. 4 (2016): 643–676.

25 See Helen Dexter, Mark Phythian, and David Strachan-Morris, "The What, Why, Who, and How of Teaching Intelligence: The Leicester Approach," *Intelligence and National Security* 32, no. 7 (2017): 920–934; Julian Richards, "Intelligence Studies, Academia and Professionalization," *International Journal of Intelligence, Security, and Public Affairs* 18, no. 1 (2016): 20–33; and Len Scott and Peter Jackson, "The Study of Intelligence in Theory and Practice," *Intelligence and National Security* 19, no. 2 (2004): 139–169.

26 See Corvaja, *The Rise of Intelligence Studies,* and Michael S. Goodman and David Omand, "What Analysts Need to Understand: The King's Intelligence Studies Program," *Studies in Intelligence* 52, no. 4 (2008).

files at CSIS.[27] As it applies to existing Canadian intelligence community members, the Canadian Association of Professional Intelligence Analysts (CAPIA) provides a platform for Canadian intelligence analysts to pursue advanced training, continuing education, and professional development.[28] However, as whole in the Canadian and British intelligence communities, academic research in intelligence studies is often seen as irrelevant, too theoretical, and ill-tuned to the needs of intelligence consumers.[29]

Studying intelligence in university, whether as a course or a program, is less important, especially outside of the United States. Intelligence agencies are generally "indifferent" to whether applicants have taken a course in intelligence; they are more interested in an applicant's area of study and they trust that basic critical thinking and analytical skills are already present. However, the real value and importance of intelligence courses lies in the fact that students who have taken courses in the subject are more likely to apply for positions in their respective intelligence community.[30]

Conclusion

The United States, United Kingdom, and Canada are at the forefront of academicization efforts concerning intelligence. In other Western countries, such as Spain, France, and Germany, the process of academicization has been slower and burdened by the darker roles played by the intelligence services at certain points in history.

In the past four decades, the distinction between two prominent approaches to the academization of intelligence has become clearer. The American approach is more influenced by the social sciences, whereas the British approach is essentially historiosophic. In contrast to the British approach, which has an emphasis on historical case studies and relies on archival documents, the American approach emphasizes theorization and a clear preference for the technical and procedural aspects of intelligence. The differences between the two schools are influenced not only by diverging academic approaches but also by the boundaries between the intelligence practitioner and the

27 Angela Gendron, "Re: Intelligence Studies in Canada," email message to Aaron Kornbluth. July 29, 2018.

28 Stéphane Lefebvre and Jeremy Littlewood, "Guide to Canadian Intelligence Issues," *Intelligencer: Journal of U.S. Intelligence Studies* 19, no. 2 (2012): 63–89.

29 Gendron, "Re: Intelligence Studies in Canada."

30 Ibid.

academic spaces. Despite the different approaches to the academization of intelligence and the divergent attitudes of the academic establishment toward the intelligence communities in the various countries, it seems that in all cases there is clear agreement regarding the importance of intelligence in foreign policy and decision-making processes.

With respect to Israel, the centrality and public awareness of security issues as well as of the general socio-military relations create a porous relationship between the security and intelligence establishments and academia. Israeli academia has a relatively plentiful presence of retired security and intelligence professionals who have rich professional experiences and vast networks of contacts. Despite that Israeli universities focus more on security issues than on intelligence per se, Israeli research in the field of intelligence studies, primarily conducted at research institutes and think tanks, is impressive and highly accessible to the public. The most prominent output on the subject of intelligence has certainly been the product of the IICC and INSS. Clearly, the singular conditions in Israel enable accelerated cooperation between the intelligence and academic communities and, with it, the significant advancement of intelligence studies in Israel. This would benefit not only the training and professional development of the Israeli intelligence community but also the Israeli academic community as obvious leaders in the field at the international level.

Forty-Five Years Since the Yom Kippur War: Intelligence and Risk Management in the Thirty Hours Preceding the War

Shmuel Even

This article examines the conduct of Israel's military leadership prior to the outbreak of the Yom Kippur War from the perspective of risk management and by looking at recently disclosed documents. From an analysis of the events, it appears that the chief of staff, David Elazar, had a clear risk management approach. On October 5, 1973, a day before the war, he put the regular army on high alert and reinforced the front lines. He did this despite the assessment of the head of Military Intelligence that the likelihood of war was extremely low. However, Lieutenant General Elazar's decision was far from being sufficient to withstand the attack that broke out the following day at 1:50 pm, in part because both he and Defense Minister Moshe Dayan failed to properly assess the risk that the regular army would struggle to contain the offensive before the arrival of reserve forces. In addition, Defense Minister Dayan and Prime Minister Golda Meir rejected the chief of staff's suggestion made the next morning to carry out a preemptive air strike against the enemies, as they were concerned about the diplomatic risk involved, which made it even more difficult for the regular army. The lessons learned from this sequence of events are that risk management is an essential part of the role of statesmen and military leaders, and the military and diplomatic risks on the strategic level should be managed jointly and should be subject to policy goals. The IDF and the other defense forces must map out

Dr. Shmuel Even is a senior researcher at INSS.

the risks involved in achieving their objectives and do what they can to reduce them—together with the political echelon—and by cooperating with them, the National Security Council, and the relevant government ministries.

Keywords: Deterrence, intelligence, Yom Kippur War, risk management, decision making, Israel

Introduction

In 2018, on the forty-fifth anniversary of the Yom Kippur War, archives in Israel released additional documents that clarify the intelligence picture and the decision-making process of the Israel Defense Forces (IDF) and the political echelon in the thirty hours preceding the Egyptian-Syrian surprise attack on October 6, 1973 at 1:50 pm. While these documents do not disclose unfamiliar events, they allow us to understand the subtleties of the intelligence information and the situation assessment. One of the more exceptional documents is a telegram sent by the head of the Mossad, Zvi Zamir, to Prime Minister Golda Meir's military secretary, in which he transmitted information given at a meeting held on October 5, 1973 in London with Ashraf Marwan. Known as "the source," Marwan was a strategic intelligence source for the Mossad and the son-in-law of Egypt's President Nasser. In the telegram, Zamir, in Marwan's name, warns about the war.[1]

This article analyzes the decision-making processes in Israel in the thirty hours preceding the Yom Kippur War from the perspective of risk management and in the context of the strategic intelligence that existed then. It does this by using original documents recently disclosed, along with information divulged in the past. The article does not aim to explain the failure of the intelligence warning—a topic that many studies and publications have discussed—but rather the way in which decision makers analyzed and understood the uncertainty and how they acted as a result.

The main figures in this event are the head of Military Intelligence, Major General Eli Zeira (September 1972–April 1974); the chief of staff, Lieutenant General David Elazar (January 1972–April 1974); the minister

1 Zvi Zamir, head of the Mossad, "Telegram to Military Secretary of Prime Minister Golda Meir, October 6, 1973," *Israel State Archives*, September 2018, https://tinyurl.com/y6shj4vw [in Hebrew].

of defense, Major General (res.) Moshe Dayan (June 1967–June 1974); and the prime minister, Golda Meir (March 1969–June 1974).

The Concept of Risk Management

Risk management is a management concept that has become increasingly common in the past few decades in the business and governmental sectors. Nonetheless, risk management itself is nothing new and has characterized business and military management from time immemorial, as will be described in this article. The concept of "risk" can be defined as the likelihood of a certain negative occurrence involving damage (loss of human life, damage to property, or not reaching objectives) for the risk-holder (person, organization, state). This concept has two components: the first is the likelihood that the occurrence will take place; the second is the amount of damage that will be incurred if the occurrence takes place. The combination of these two components allows for assessing the intensity of the risk (the "expected loss").

Risk management aims to reduce risks or improve the risk-benefit ratio. The decision maker takes risks in order to exploit opportunities and also in order to reduce the cost of an error. Risk management in organizations is a methodical process in which risks are identified, mapped out in advance, ranked according to their expected loss, and the probability of the risk. This process also includes a plan for reducing risks, as well as for continuing to function in case of negative occurrences. Risk management exists even when its methodology has not been formally adopted but is inherent in activities of defining and mapping out risks, conducting research and gathering information for the purpose of assessing the probability of the risk and the possible loss; diversifying risks; reducing risks for which the loss, if they occur, will be great, even if the probability of their occurrence is low; strengthening weak links in critical processes; balancing between different risks by transferring resources to lower the most severe risks; taking steps to reduce the impact of uncertainty by hedging risks, preparing alternatives, maintaining stockpiles and resources for emergencies; and improving response capability and speed for unexpected events. Risk management can have costs, whether as a result of activities such as these or due to the possibility of errors in formal risk management. This in itself is a risk.

Strategic-security risk to the State of Israel can be defined as the possibility of an occurrence, such as a war, which could harm the population, property,

the state's sovereignty, and/or its image. The defense forces—primarily the IDF—are entrusted with lowering security risks by deterring the enemy from engaging in hostilities, and they are tasked with bringing victory if the risks materialize. From the perspective of the defense forces, the main risk is the failure to achieve the goals and objectives that the political echelon has determined for them. Given the extent of the potential loss from strategic-security risks, security-risk management is meant to support the carrying out of actions designed to lower risks, even in situations where the risk probability is not high.

Managing the Risk of an Arab Attack Prior to the Eve of the Yom Kippur War

The main military risk that Israel faced from its establishment until at least the Six Day War was a large-scale invasion by the Arab armies. This risk, which was seen as an existential one, first materialized in the War of Independence in 1948 and took a heavy toll on human lives. After the war, Israel recognized that the economy's workforce could not be permanently enlisted, and that this risk had to be managed subject to the constraints of the resources and in consideration of the civic goals of the nascent state, which faced difficult economic conditions and the task of absorbing mass immigration.

Prime Minister and Defense Minister David Ben-Gurion extensively analyzed this issue in a strategy document that he had prepared in 1953.[2] The document expressed his security doctrine and should be seen as a formative document for the framework of managing the security risks that Israel faced.[3] In the document, Ben-Gurion stated that Israel should manage the risk of an invasion by Arab armies by having a small regular army based on conscripts and career soldiers and a large reserve army that would be called to war upon receiving advanced warning, which intelligence should provide. In this way, Israel attempted to balance between the external risk posed by the enemy and the internal risk that an invasion posed to the country's social and economic stability.

2 David Ben-Gurion, "Army and State," memorandum submitted by the Prime Minister and Defense Minister David Ben-Gurion to the government, October 18, 1953, *Maarchot* no. 279–280 (June 1981) [in Hebrew].

3 Isaac Ben Israel and Nicki Kons, "Ben-Gurion's Approach to Risk Management," *Maarchot* no. 452 (December 2013) [in Hebrew].

As a result of the security doctrine that Ben-Gurion had formulated, and despite the constraints, Israel succeeded in building a strong army that achieved victories in the Sinai Campaign in 1956 and the Six Day War in 1967. These events demonstrated another important element of risk management at that time, which was engaging in an offensive initiative as part of the security doctrine. Israel decided that it could not wait behind its defensive lines along its borders for the Arab armies to attack, but rather, it would preempt them. The offensive initiative aimed to thwart enemy attacks, to keep the war away from Israel's civilian population, to exploit the IDF's advantages of mobility, and to surprise the enemy. The alternative of waiting for a ground attack by an enemy army was considered a much greater risk. However, preemptive attacks had diplomatic risk as well; in the international arena, Israel risked being accused as the aggressor and of not receiving the support of the superpowers. This risk led to difficult deliberations within Israel's political echelon prior to launching the preemptive attack on June 5, 1967. In that instance, the military risk was weighed against the diplomatic risk; in the end, the army's high level of readiness, the heavy pressure on the senior officers, and a last-minute update on the US position tipped the scales in favor of the preemptive strike.

The beginnings of the Yom Kippur War can already be seen in the conclusion of the Six Day War. The Arabs did not accept the results of the 1967 war, while Israel sought to protect its achievements. Following the Six Day War, the territories under Israel's control grew more than fourfold, and the IDF needed to also defend the "territories held,"[4] until the political echelon decided their future. This was a complex challenge: On one hand, Israel won strategic depth on three fronts—in Sinai, the West Bank, and the Golan Heights, while on the other hand, the IDF was required to deploy forces and logistics over large areas and had to rule over the population in the newly added territories. This led to a significant increase in defense spending. In 1971–1972, defense spending amounted to an annual average of 20.5 percent of GDP, compared to 9.2 percent on average during the years 1965–1966.[5]

4 "Protocol 159 of the Constitution, Law and Justice Committee," *The Knesset*, December 25, 1967. In this meeting it was decided to adopt the concept of "the territories held by the Israel Defense Forces," https://akevot.org.il/wp-content/uploads/2016/11/1967-12-25-Shamgar.pdf [in Hebrew].

5 Central Bureau of Statistics, "Defense Spending 1950–2015," no. 1680 (May 2017) [in Hebrew].

The strategy changed in the years following the Six Day War: The IDF moved from a strategy of a preemptive strike using multiple branches of the armed forces to a strategy of a defensive position at the new front lines. These front lines had serious limitations, however, given the possibility of an all-out attack. At the Suez Canal front, a defensive line was established (the "Bar Lev Line"), which included sixteen manned outposts (*maoz*) on the front line, and next to them outposts at a depth of ten kilometers (*taoz;* plural *taozim*). There were many kilometers between each *maoz*, such that the defensive line was not continuous. The combat method was based mainly on armored forces that were stationed along the line of the *taozim* and east of it. The standing force in Sinai consisted of Division 252 (the "Sinai Division"), and its defensive plan ("Dovecote") was meant to handle limited enemy scenarios: opening fire along the front line, Egyptian attempts to capture IDF outposts on the canal line, and commando operations in Sinai. According to the plan, the Southern Command had to prepare to repel any Egyptian crossing attempts in western Sinai and in the Shlomo District (southern Sinai).[6]

In the Golan Heights, the strategic defensive depth was more limited and the border was close to population centers The regular force included only two infantry battalions along the border, two tank battalions, and an artillery battalion. Before the war it was reinforced by an additional tank division and more than two artillery battalions.

In May 1973, following the assessment of the military leadership—with the exception of the head of Military Intelligence—that war was about to break out at Egypt and Syria's initiative, the IDF went on alert and began its preparations for war, which included setting up new units and preparing operational plans (under the code name "Blue-White Alert"). Since the war did not occur on the estimated date, this assessment was mistakenly seen as a "false alarm,"[7] which bolstered the position of the head of Military Intelligence as the one person who had assessed that war would not break out. In retrospect, after the Yom Kippur War, it was learned that the Egyptians and Syrian had

6 Southern Command, "Dovecote Order, Summary," December 17, 1972, *IDF Archive*, 1984; website of the 14th Armored Brigade, https://tinyurl.com/y5maf858 [in Hebrew].

7 False alarm for war is an unjustified alert that involves a rise in the risk of deteriorating into a war that neither side wants, the attrition of the defense forces, and social costs (recruitment of reserves), as well as economic and diplomatic costs.

indeed intended to attack in May 1973, but the date had been postponed to October 1973.[8] Thus, in effect, the Blue-White Alert was justified and Major General Zeira, the head of Military Intelligence, was mistaken then too. Although the Blue-White Alert contributed to the IDF's preparations for the Yom Kippur War, the fear of false alarms became a concern that negatively influenced the risk management prior to the outbreak of war.

On October 1, 1973, at the General Staff's situation assessment, the head of Military Intelligence indicated a unique situation vis-à-vis Egypt and Syria. He claimed that "in Egypt a major exercise at the General Staff level is beginning today, accompanied by the movement of armored divisions, bridging units, paratroopers, and airborne units on an exceptionally large scale. All this is taking place as part of the Tahrir 41 exercise, and there is no intention to turn this into war." Adding that the Syrian Army was also engaging in an unprecedented emergency deployment, Major General Zeira reassured that "since it does not appear that Egypt is going to war, this means that Syria too will not go to war." In retrospect, it became clear to Israel that Tahrir 41 was a central component of Egypt's deceptive plan to launch the Yom Kippur War; the preparations for the attack were carried out through the exercise, while the transition to war itself occurred by means of a code word.[9]

Until October 5, 1973, despite the increasing deployment of forces on the Egyptian and Syrian fronts, Israel did not manage concrete risks and this apparently was due to three reasons: It had accepted the intelligence assessment that seemingly provided explanations for the unusual military activity (exercises, fear of Israel); Israel assumed that if the enemy decided to go to war, it would receive advanced warning of this, as the head of Military Intelligence had promised (for example, in the cabinet on April 24, 1973);[10] and it was assumed that the IDF's regular army could contain the attacking

8 Yoel Ben-Porat, "Endnote: The Yom Kippur War, Mistake in May and Surprise in October," *Maarchot* no. 302–303 (April 1986) [in Hebrew].

9 Aharon Ze'evi, "Egypt's Deception Plan," *Maarchot* no. 289–290 (October 1983) [in Hebrew].

10 Uri Bar Yosef, "The Surprise of the Yom Kippur War and its Sources," *Maarchot* no. 361 (November 1998) [in Hebrew] (based on the Agranat Commission Report on April 1, 1974).

forces until the arrival of reserves, as the chief of staff had promised.[11] These assumptions appeared to be compatible with the risk management framework up until that time.

Risk Management the Day before the Outbreak of the War (October 5, 1973)

On the night between October 4 and 5, 1973, the intelligence picture changed dramatically. In a surveillance sortie that took place in the afternoon and was deciphered at night, it was discovered that the Egyptian army had fully prepared its emergency formations and that the armored and artillery units at the various levels, including at the General Staff level, were deployed in their positions on the front line.[12] That night, Military Intelligence received information that the families of Soviet advisors were being evacuated from Syria and Egypt without explanation. At 2:30 am that same night, the head of the Mossad, Major General (res.) Zvi Zamir, received a message that the important intelligence source, Ashraf Marwan, wanted to meet with him right away. Marwan's message included the use of a code word that was a signal for war. The head of Military Intelligence and head of the Mossad updated one another.[13]

On October 5, 1973 at 8:20 am, the chief of staff held a consultation in his office (around thirty hours before the Egyptian-Syrian surprise attack). The head of Military Intelligence opened by stating, "The basic assessment that the Arabs are afraid and will not go to war has not changed." The head of Military Intelligence did not have an explanation why the Soviets were evacuating the families of advisors, but estimated that if they believed that the Arabs were going to attack Israel, they would contact the United States, and it would contact Israel, and then "we would know what was happening."

11 Hagai Tsoref, conversation with Aharon Barnea, in honor of the publication of the book he edited, *Golda Meir, the Fourth Prime Minister*, "Hayu Yamim" program, *Knesset Channel*, September 21, 2016, https://www.youtube.com/watch?v=4yziTBtBsfg [in Hebrew].

12 Yossi Barkan "Things that I Saw There," *Mabat Malam* no. 82 (October 2018) [in Hebrew]. The author was the head of the Egypt Department in Southern Command Intelligence during the Yom Kippur War.

13 Shimon Golan, "All the Signs Were There," *Yisrael Hayom*, September 13, 2013. This article was excerpted from the book *War on Yom Kippur – Decision-making in the Senior Command during the Yom Kippur War*, published by Modan and Maarchot, 2013 [in Hebrew].

The head of Military Intelligence informed that Zvi Zamir, the head of the Mossad, was expected to receive information from a reliable source about a "warning of war."

The chief of staff said in that meeting that "Basically I do not suppose that they are going to attack, but there is no proof that they are not going to attack, so elementary preparations are necessary. Therefore, we decided on the cancellation of leave in the armored forces and now in the air force." The deputy chief of staff, Major General Israel Tal, added that "Tonight all leave was cancelled and all of the tanks were equipped." The chief of staff supported the air force's recommendation to continue sorties for aerial photographs. In his opinion, this could deter the enemy (if it indeed intended to carry out a surprise attack).[14]

On October 5 at 9:00 am, the regular weekly discussion led by Minister of Defense Moshe Dayan began. The chief of staff said in the discussion that it was impossible to know with certainty whether the steps taken by Egypt and Syria were the result of fear of IDF actions, or if their purpose was offensive. According to the chief of staff, if he were not in a position that required him to make decisions, "I would say that it is not an attack," but as the chief of staff, he stated that "I need to think about whether I have proof that there is not going to be an attack. I do not have proof that it is not going to be an attack." Therefore, he ordered the cancellation of leave on both the Egyptian and Syrian fronts and in the air force, and the reinforcement of the two fronts with standing forces.

The head of Military Intelligence emphasized in the discussion that the most worrisome development was the evacuation of the Soviet families. He claimed that this was not sufficient for changing the basic intelligence assessment that Syria and Egypt did not intend to attack, stating, however, that "it raises some doubts for me, and it is certainly justified to do what the chief of staff spoke of." He stuck with his assessment that the enemy's preparations stemmed from a fear of Israel. In addition, Major General Zeira reported that the head of the Mossad had received warning that night that

14 "Summary of the Situation Assessment at the Chief of Staff's Office, October 5, 1973, 8:25 AM" *IDF Archive*, 2018, quoted in Gadi Zohar, "One Discussion on October 5," in "45 Years Since the Yom Kippur War," special issue, *Mabat Malam* no. 82 October 2018, p. 50, https://tinyurl.com/y6xzgr42 [in Hebrew].

"something is going to happen" and that he was planning to meet with "the source" (Ashraf Marwan) that night, October 5 at 10:00 pm.[15]

The defense minister said to the chief of staff that "For Yom Kippur, everything that you did is good and right." He asked to consider the possibility of announcing in advance over the radio that people should listen to the Army Radio broadcasts during Yom Kippur, so that it would be possible, if necessary, to gather reserve forces and transport them to the front lines that same day. Dayan decided to recommend to Prime Minister Meir to contact the Americans with the following information: 1) The assessment in Israel was that the likelihood of an Arab attack was higher than previously estimated; there was various indications that Egypt and Syria were preparing for an offensive attack; and it was possible that the exercise in Egypt was camouflaging an intention to attack; 2) Could they find out whether the Arabs indeed intended to attack and that Israel promised that it did not have any offensive intentions. According to Dayan, Israel would then decide how to act after receiving the Americans' response. The defense minister also asked to check if it would be necessary to request equipment immediately from the United States if it did confirm the indications that the Arabs were intending to attack.[16]

On October 5 at 10:00 am, a consultation began at the Prime Minister's Office at the IDF Headquarters in Tel Aviv. The head of Military Intelligence said that an Egyptian-Syrian attack was "very unlikely," but perhaps the Russians thought (mistakenly) that the Arabs were about to attack, since they did not know them well enough. Major General Zeira noted that Military Intelligence had assessed that the preparations and activities of the Egyptian and Syrian armies were mainly due to fear of Israeli actions, but it was impossible to ignore the evacuation of the Russian families, the meaning of which was unclear. The chief of staff reported on the steps of preparedness and reinforcement that he had taken, as a result of the lack of positive proof that Egypt and Syria did not intend to go to war on one hand, and from the ability of the armies of the two countries to strike on short notice on the other hand. However, he calculated that Egypt and Syria did not intend to attack and that "if they are going to attack—we will receive better indications."

15 Golan, "All the Signs Were There."

16 Ibid.

The defense minister suggested to contact the Americans, to report to them that there were indications of a possible Arab attack that was more realistic than in the past, to ask them to contact the Soviets and send them the message that Israel did not have any offensive intentions, and to warn them that if the Arabs started a war, they would "get cold water." The prime minister said that it was possible that the meeting of the UN General Assembly was spurring the Arabs to demonstrate activity and motivating them to take action. She accepted the defense minister's recommendation to contact the Americans and his suggestion to notify additional ministers about the information on the recent developments.[17]

On October 5 at 12:30 PM, a discussion of the General Staff began, led by the chief of staff and with eleven major generals present. The minutes of the meeting were published in October 2018.[18] The head of Military Intelligence reported on the emergency preparations of the Syrian Army starting on September 5, 1973 and on its exercise of conquering the Golan Heights according to the attack plan. He also reported on the advancement of two air force attack squadrons close to Damascus, which would improve their ability to attack deep into Israel. Major General Zeira said that in Egypt, a large-scale military exercise was taking place; the canal area was reinforced with 300 artillery guns; and many tanks had been brought closer to firing positions along the canal. He estimated that the activities of the Egyptian and Syrian armies were out of defensive motivations, due to a fear of Israel. The head of Military Intelligence noted a series of unusual events: the arrival of eleven Soviet transport aircraft in Egypt and Syria, possibly in order to remove "Russian personnel" from those countries, and the evacuation of the Soviet vessels from the Port of Alexandria. Nonetheless, he concluded his assessment by saying that the likelihood of war was "low, and even lower than low."[19]

The chief of staff, although he seemingly accepted the Military Intelligence's assessment, actually calculated it differently: "I see the danger that war will break out today or tomorrow as being less likely than that of war not occurring." He added, "I do not think that this is 'zero hour' for this evening

17 Ibid.

18 "Minutes of the General Staff Discussion that Took Place on October 5, 1973," *Archive of the IDF and Ministry of Defense*, October 2018, https://tinyurl.com/yxfup23u [in Hebrew].

19 Ibid.

or tomorrow, and if this is their intention and they have a 'zero hour,' I hope that we will receive advance warning." Lieutenant General Elazar noted that "the defensive formation is certainly also an offensive formation" and that "we do not have positive proof that they are not going to attack," and added, "If I were a commentator, I would put a period here and say that I do not think that it is going to happen. Since we are not only commentators, but responsible for the situation, we have to take the necessary security measures, and we are indeed taking them." In his words, "If the worst possible situation happens, that is if they attack without another word, then we will have to contain them using the standing forces. That means using the air force and all of the forces that we have on the front lines. To this end, we are not only declaring a state of alert [level] 3,[20] but also reinforcing the front lines with standing forces that we have in Israel." The chief of staff also announced that they were checking how to call up reserves on Yom Kippur (without listening to the radio) "in case of a catastrophe."[21] Following this, the Army Radio prepared for the possibility of having to broadcast on Yom Kippur. At the end of the discussion and given the steps decided upon, Lieutenant General Elazar said that if war occurred that day, it would no longer be a "complete surprise" but an "almost complete surprise," and the war would start with "opening conditions that are not exactly preferable."[22]

Analysis of the Risk Management on October 5, 1973

Concrete risk management began on October 5, considering the change that occurred in the intelligence picture. This process was apparent, first and foremost, with the chief of staff, who began making decisions under conditions of considerable uncertainty, which meant he lacked a warning of war based on intelligence. The most significant steps taken were raising the alert to the highest level in the regular army and reinforcing the front lines. The cost of these decisions was significant, and at the time there was seemingly concern that they contributed to the risks of deterioration, considering the Military Intelligence's assessment that the enemy's actions resulted from

20 The highest state of alert in the standing army, without large-scale recruitment of reserves.

21 "Minutes of the General Staff Discussion that Took Place on October 5, 1973."

22 Ibid.

the fear of the IDF. Important steps, whose costs were low, were also taken, such as the preparations of the Army Radio to broadcast on Yom Kippur.

The way in which the chief of staff managed risks clearly had accelerated: If on the morning of October 5, he decided to augment the forces on the front lines using standing forces within Israeli territory, in the afternoon he had already placed the regular army on high alert level 3. However, the chief of staff did not cross the line of recruiting reserves, which required the approval of the political echelon.

The following factors seem to have influenced the chief of staff to begin managing risks:

a. **Erosion of confidence in the assumption that the head of Military Intelligence would provide a concrete advanced warning.** It became clear that Military Intelligence had been surprised and was unable to provide convincing explanations for significant events, such as the evacuation of the Soviet families from Syria and Egypt and the Egyptian army's full emergency preparations on the Suez Canal front ("Tahrir 41" was defined, as noted, mainly as a command exercise). Although the chief of staff continued to hope that he would receive advanced warning from intelligence, he already began speaking about the possibility of not having any advanced warning. He began to act not only on what he knew but also on what he knew that he did not know.[23]
b. **Substantial shift in the assessment of the likelihood that war would break out.** The chief of staff and head of Military Intelligence seemingly agreed that war would not break out, but the range of likelihood that they attributed to the outbreak of war was substantially different. While the head of Military Intelligence estimated that the likelihood of war was "lower than low," which can be interpreted as only a remote possibility, slightly above zero, the chief of staff estimated that the likelihood of war was less than the likelihood that war would not break out, which can be interpreted as a likelihood in the range of under 50 percent.
c. **Drastic reduction of the "advanced warning timespan,"** referring to the time from the moment advanced warning is received until the outbreak of war. According to the chief of staff, the minimal advanced

23 Shimon Golan, "The Advanced Warning on the Eve of the Yom Kippur War – Military Intelligence's Assessment and the Basis for the Leadership's Decisions," *Mabat Malam*, 67 (November 2013) https://tinyurl.com/yyycvr7q [in Hebrew].

warning timespan necessary for recruiting the reserves before the onset of an enemy attack was at least twenty-four hours.[24] Since the enemy forces were already prepared in territories that enabled them to attack (also according to the assessment of the head of Military Intelligence), the advanced warning timespan that could have been expected from intelligence was significantly reduced and was insufficient for recruiting the reserves.

Behind all of these factors was Lieutenant General Elazar's exceptional recognition that risk management was an integral part of the role of the chief of staff. In this respect, the distinction that he made between the positions of a commentator and chief of staff as commander in-chief is interesting. It shows that his expectation of commentators was to provide a binary assessment (either war will take place or not), whereas the commander in-chief's professional assessment required operating also in situations of uncertainty, even if the situations went against the prevailing assessment and even if that assessment was shared by the chief of staff himself.

The political echelon manifested its risk management in its decision to contact the United States in order to create a shared understanding and send a message to the enemies. This idea seemed correct in terms of diplomacy and also because it could have (ostensibly) lowered the risk of a surprise attack, or alternatively it could have justified a preemptive response by Israel. Although the cost of this step was not high, in practice, it happened too slowly and too late and did not achieve its objective.

Henry Kissinger, then the US secretary of state, later explained that he did not see the urgency in passing on the message that he had received from Israel until the moment that the assistant secretary of state, Joseph Sisco, sent him a message about the imminent war on October 6, close to 1:00 pm Israel time (less than an hour before the attack). Only then did Kissinger call the Egyptian foreign minister, and Soviet and Syrian ambassadors in Washington; the latter did not answer him. Regardless, according to Kissinger, the wording of the message that Israel had asked him to pass on to the Arabs was "that Israel does not intend to carry out a preemptive strike."[25] That is,

24 "Summary of Consultation with the Prime Minister, Tel Aviv, Yom Kippur 1973 at 8:05 AM," *Israel State Archives*, October 2010 [in Hebrew].

25 Amir Oren, "Henry Kissinger: You Know We Saved You in '73, Right?" *Haaretz*, October 4, 2013 [in Hebrew].

the message was meant to prevent an Arab miscalculation regarding Israel's intentions, but it did not deter them from attacking.

Did the initial message of warning from the Mossad's intelligence source have any impact? It is hard to discern any impact that the message, which contained the code word for war, may have had on decision makers on October 5, 1973. Brigadier-General (res.) Gadi Zohar, who had served then as adjutant to the chief of staff, noted later that the report on the message was shared in the three discussions mentioned above without any reaction, nor did they mention the "special sources" of which everyone knew.[26] That is, the code word for war did not influence the intelligence assessment and it is doubtful whether it was expressed in the risk management, until the report of Zvi Zamir, the head of the Mossad, was received on October 6.

Furthermore, the fact that the cabinet waited to receive a full report that night may have been a factor that delayed the risk management at that time, since there is a natural tendency to wait for additional information that will dispel uncertainty, especially when considering the weight of the decisions and the cost of a mistake. The defense minister's approach that Israel should wait for a response from the United States in order to decide how to act could have also been a factor in delaying the decision making.

Risk Management on October 6, 1973

On Yom Kippur, October 6, 1973 at 4:30 am, Chief of Staff Elazar received an initial report about the meeting of the head of the Mossad, Zvi Zamir with the "source," Ashraf Marwan on October 5 in London.[27] The main message of the report was that at 6:00 pm, an Egyptian-Syrian attack on the State of Israel was to begin. Later that morning at 7:25 am, Zamir sent a detailed telegram.[28] According to the telegram, "The Egyptian Army and the Syrian Army are about to start an attack on Israel on Saturday October 6, 1973 in the early evening."[29] The likelihood of the attack was estimated by Marwan to be 99 percent! The "source" shared how the Egyptian attack

26 Zohar, "One Discussion on October 5," p. 50 [in Hebrew].

27 "Chief of Staff's Log, 1973," *Archive of the IDF and Ministry of Defense*, May 2019 [in Hebrew].

28 Zamir, Telegram to Prime Minister Golda Meir's Military Secretary on October 6, 1973 [in Hebrew].

29 In actuality the time of the coordinated attack was moved forward from 6:00 pm to 1:50 pm.

was to be implemented, including the intention to carry out a strategic stop after conquering ten kilometers from the eastern bank of the canal—an important piece of information that the IDF did not internalize even after the war had broken out. According to the telegram, on October 3, 1973, Marwan himself had arranged for the transfer of Egyptian navy vessels and Egyptian civilian aircraft from Egypt to Libya, so that they would not be damaged in the war—additional evidence of the intelligence source's accessibility. Zamir also wrote that given the tight timeline, the "source" had suggested publicizing Egypt's intention to go to war, in order to eliminate the element of surprise that Egypt had planned and to deter them from carrying out the attack. The head of the Mossad supported Marwan's suggestion.[30]

According to the chief of staff's log from October 6, 1973, which was recently disclosed, **at 5:30 am,** the chief of staff held a short meeting with the heads of the IDF's directorates, the major generals of the regional commands, and the branch commanders. **At 5:50 am,** a discussion was held with the defense minister, Moshe Dayan. **At 7:15 am,** the chief of staff held another meeting with the heads of the directorates, the major generals of the regional commands, and the commanders of the branches. The chief of staff said that given the intelligence information, he assumed that at 6:00 pm that day the attack would begin. He ordered the air force to prepare for a preemptive strike on the Syrian front in the afternoon but noted that at this stage, the defense minister opposed a preemptive strike.[31]

On October 6, 1973 at 8:05 am, a crucial meeting was held with Prime Minister Golda Meir. The meeting began, strangely, with two suggestions from the defense minister: to not prevent the Arabs from the territories from working in Israel; and to order the evacuation of the children from the Israeli communities in the Golan Heights (thirty children), from Abu Rudeis, and from the Shlomo District. Prime Minister Meir suggested that the children be evacuated immediately and not on the eve of the action, and the chief of staff corrected her and said, "We are already on the eve of the action."

30 Zamir, Telegram to Prime Minister Golda Meir's Military Secretary on October 6, 1973 [in Hebrew].

31 "Chief of Staff's Log, 1973," *Archive of the IDF and Ministry of Defense*, May 2019 [in Hebrew].

Afterwards the discussion moved to the strategic level and centered on the letter of the head of the Mossad.[32]

In the meeting, the head of Military Intelligence said, "Despite the fact that they are prepared, in my opinion they know that they will lose. Sadat is not in a situation today in which he has to wage war, everything is ready, but there is no necessity, and he knows that the balance will not improve […] he has not yet given the order to go to war. It is possible that by the last moment he will be deterred. Perhaps we can affect what he will do or decide." Major General Zeira supported the suggestion to contact the United States and warn Egypt by way of the Americans.

The chief of staff remarked that "at night the Syrians brought forward their medium artillery, meaning that they are on the attack and not on the defense." In relating to Zamir's letter on the Egyptian attack, Lieutenant General Elazar stated that "for us this is very short notice. If they attack in ten hours, we are maximally prepared with the regular army. But we have not recruited reserves at all. The IDF's might is 25 percent regular army and 75 percent reserves." His recommendations were to recruit 200,000 reserve soldiers and carry out a preemptive air strike. According to Elazar, "a preemptive strike is of course a huge advantage. It will save many lives. If we enter a war in which the first stage is containment—and I have confidence that we will handle it—and then attack, it will be a serious war."[33]

The political echelon only partly accepted the chief of staff's recommendations. The defense minister believed that only limited reserves should be recruited, so that Israel would not be accused of aggression, in addition to internal considerations ("do we need to create a mood of war?"). During the discussion, the chief of staff agreed to the recruitment of 100,000–120,000 reserve soldiers, although Defense Minister Dayan suggested recruiting fewer than half of this number. The prime minister believed that the extent of recruitment that the chief of staff had requested would have had the same diplomatic effect as what the defense minister had suggested, and thus it was decided that the chief of staff would determine the number.

Both the prime minister and defense minister rejected the chief of staff's suggestion regarding a preemptive air strike out of concern that Israel would

32 "Summary of Consultation with the Prime Minister, Tel Aviv, Yom Kippur 1973 at 8:05 am."

33 Ibid.

be accused of being responsible for the outbreak of the war.[34] It should be noted in this respect that the air force was ready to strike airfields in Syria toward 11:00 am, but as mentioned, the political echelon did not approve carrying out the attack.[35] Golda Meir supported the suggestion made by the "source" and the head of the Mossad to publicize (through foreign news agencies) the possibility of an Arab attack, in order to eliminate the element of surprise from the attack and perhaps even thwart it.

The question of Jordan joining the war hovered in the air. Considering the circumstances, this would have been a considerable military risk to Israel. Nevertheless, the minister of defense suggested that they not warn King Hussein about joining the war. The minister of defense did say, however, that Israel would bomb radar stations in Jordan should they be used to provide the Egyptians with an aerial picture of Israel.[36]

Later in the morning and in the afternoon, the defense minister and the chief of staff engaged in intensive staff work to prepare the IDF to contain the Egyptian-Syrian attack on October 6 at 5:00–6:00 pm. According to the chief of staff, the IDF's order of battle to contain the attack at that time amounted to 180 tanks on the Golan Heights and 300 tanks facing the Suez Canal.[37]

Analysis of the Risk Management on the Morning of October 6

The warning telegram from the head of the Mossad, Zvi Zamir, which, as already mentioned, was received on the morning of October 6, led to a change in the situation assessment. Questions as to why this information was not received earlier,[38] and why Israel's preparations for war were not accelerated, beyond what was done, from the moment Zamir's report was received at 4:30 am remain unanswered. Regardless, following the arrival of the warning, the political-military leadership had to make decisions and

34 Ibid.

35 Yossi Aboudi, "War from the Air: The Intelligence that Helped the Air Force Take Off," *Mabat Malam* no. 67 (November 2013), p. 54, https://tinyurl.com/y4qjrhrh [in Hebrew].

36 "Summary of Consultation with the Prime Minister, Tel Aviv, Yom Kippur 1973 at 8:05 am."

37 Detailed in "Chief of Staff's Log, 1973," *Archive of the IDF and Ministry of Defense*, May 2019.

38 Zohar, "One Discussion on October 5."

take risks. The willingness of each member of the cabinet to take operative steps could indicate their level of understanding of the seriousness of the risk of war and their approach to risk management at that time.

Despite the clear warning, the head of Military Intelligence still tried to impose his logic upon the enemy and explained that war was not worthwhile for Egypt's President Sadat, and thus it might not occur. In effect, the head of Military Intelligence did not understand the reasoning and the purpose of the Egyptian attack to conquer the Eastern bank of the Suez Canal in order to bring about a diplomatic process. The lesson is that understanding the reason for the risk does not have to be a necessary condition in order to prepare to handle it.

The chief of staff was the only one who understood the risk of war. He was less troubled by the question of the reasons behind the Egyptian attack. His understanding of the risk was based on an analysis of the enemy's situation and the learning process that he had undergone since the previous morning. It seems that he saw in Zamir's report the concrete warning that he had been waiting for. The outline of the war also became clearer to him from the report—it was not the "heating up" of the border but rather a major attack on two fronts—and the steps that he took the day before were far from sufficient to address the risk. Now he demanded the full recruitment of reserves and approval for conducting a preemptive air strike in order to disrupt the attack on both fronts before it had even begun.

Defense Minister Dayan was less ready to make decisions to lower the risk posed by the war. He chose to limit the military steps that the chief of staff suggested, as he was concerned that the State of Israel would risk being perceived as the aggressor and he was also worried about hurting the country's morale. If not for the prime minister, Defense Minister Dayan would have dictated to the chief of staff a more limited recruitment of reserves (only two divisions, as opposed to the four divisions suggested by the chief of staff). In parallel, both Golda Meir and Moshe Dayan prevented the chief of staff from conducting an Israeli preemptive air strike out of concern for the diplomatic risk, which in turn would increase the risk to the regular army. As far as we know, this matter was not brought up in any of the meetings.

The Materialization of the Risks

On October 6, 1973, Yom Kippur, at 1:50 pm, the Egyptian-Syrian attack began, and Israel's defensive lines along the Suez Canal and in the Golan Heights were breached along their entire length. It quickly became clear that the emergency warehouses were not properly prepared, which made it even harder to organize the reserves.[39] Nevertheless, the recruitment of the reserves was successful, primarily due to the soldiers' determination to reach the front lines.

At the end of Yom Kippur that evening, Minister of Defense Moshe Dayan appeared on Israeli television and reported to the nation about the state of the war. He stated that starting at 1:50 pm, Egypt and Syria had begun a simultaneous attack on two fronts, in the Sinai and the Golan Heights respectively. Regarding the Syrian front, Dayan said that in the Golan Heights "perhaps here and there several tanks have penetrated beyond our lines. Perhaps also they captured some of our positions, [but they are] not significant conquests." As for the Egyptian front, Dayan said that "the Egyptians have succeeded in crossing the canal in certain places, and we have suffered losses of soldiers and positions. But relatively speaking, this is more or less as we expected the first day of the battle to be, the same battle that will end with our victory in the coming days."[40] This description by the defense minister—whether it resulted from the fog of war or whether it was intended to calm the public—was exceedingly far from reality. Later in his address, Dayan sought to explain why the considerations of Israel's leadership were correct—in that Israel had sustained an Arab attack and did not counterattack. He said that Israel did not want to start a preemptive war as it did not want to get caught in a situation where it would be accused of instigating the war. Dayan explained that the alternative to the path that Israel took was to keep an exceedingly large number of soldiers on the front lines for years and to carry out a preemptive strike every time that there was

39 "The Yom Kippur War – the Story from the Ordnance Corps' History Book," *Technology and Maintenance Corps Association Website*, March 2019, https://tinyurl.com/y5uwocyy [in Hebrew].

40 Moshe Dayan, appearance on Israeli television on October 6, 1973, in "Forty-five Years Since the Yom Kippur War, Looking Back," *Kan 11 Television Channel*, October 7, 2018 [in Hebrew].

concern that the enemy intended to start a war, a move that would depict Israel as the aggressor.[41]

The defense minister's description on television seemingly showed that the situation on the front lines matched the leadership's expectations according to the Israel's security doctrine and was consistent with its risk management framework. But in reality, its risk management had failed: Warning was not received in time; the recruitment of reserves occurred late; Israel did not conduct a preemptive air strike; the defensive lines of the regular army were breached; and the uncertainty was immense.

On October 7, 1973, in a meeting held in the morning, Golda Meir basically admitted that she had made a mistake by not allowing a preemptive strike as the chief of staff had requested. She said, "If, God forbid, we are ever in such a situation again, we need to disregard the world and let the army attack."[42] Although the defense minister was not present at this particular meeting, at the meeting that afternoon he too admitted his mistake on the eve of the war, saying, "I underestimated the strength of the enemy, his belligerent magnitude, and I overestimated our forces and their resilience."[43] In these words, Dayan made a distinction between surprise at the enemy's capabilities (the intelligence surprise) and at the IDF's lack of resilience at the onset of the war (operational surprise); Dayan was shocked at both. Dayan also surmised that the "war is about the Land of Israel," meaning not only about the "territories." At that time, his risk assessment of the war shifted from one extreme to the other.

Golda Meir was also shocked by the results at the beginning of the war. Dr. Hagai Tsoref, director of documentation and commemoration at the Israel State Archives, later said that the minutes from the meetings held with the top military echelons indicate that the prime minister was not surprised by the outbreak of war. According to Tsoref, Prime Minister Meir certainly thought before the war that a war could break out, even on Yom Kippur, but she was stunned by the terrible results of its first few days. Throughout all the discussions Meir held with the military leadership prior to the war, she received promises mainly from the chief of staff that in any situation, the

41 Ibid.

42 "Minutes of Discussion with the Prime Minister in October 1973, 9:10 am," *Israel State Archives*, October 20, https://tinyurl.com/y2nonk94 [in Hebrew].

43 "Minutes of Discussion with the Prime Minister in October 1973, 1:40 pm," *Israel State Archives*, October 2010, https://tinyurl.com/y662sr22 [in Hebrew].

IDF's regular army would be able to contain the attack, while recruiting the reserves was important mainly for the counterattack, and not for defense.[44]

As the war progressed, Israel took some other high risks, such as leaving the border with Jordan almost undefended, in the assumption that Jordan would not join the war (a risk that justified itself); the failed counterattack in Sinai on October 8; and the decision to cross the canal in the middle of December (Operation Abirey Ha-Lev), which led to the war's reversal in Israel's favor.

The Main Risks and Their Management in Retrospect

The risk of a surprise attack

Although the Israeli leadership had considered the risk of an Arab attack before the war, it suffered from being overconfident in Israel's strength, while it underestimated the determination and strength of its opponents; that is, the war itself was not a surprise and the leadership even took it seriously (for example, in the Blue-White Alert). However, the leadership had little awareness of the risk that war would break out by surprise, because the cabinet was confident that the Military Intelligence would fulfill its role and provide warning so that at least they would be able to recruit the reserves. As a result, without having received any prior warning from Military Intelligence, the outbreak of the war was met with shock not only by the head of Military Intelligence Eli Zeira, but also by the Defense Minister Moshe Dayan.

In contrast, Chief of Staff David Elazar was less surprised, because he had engaged in risk management. On October 5, he already had considered that the likelihood of the risk of war was real and required taking operative steps even without warning from Military Intelligence. Following the report of the head of the Mossad on the morning of October 6, the chief of staff understood that he had received the concrete warning that he had expected earlier, and the outline of the war became more apparent to him. At that point, he also understood the intensity of the risk and adjusted his orders accordingly, but they were given too late. In the end, the risk materialized and its management was inadequate.

44 Tsoref, conversation with Aharon Barnea.

The risk of a false alarm

The awareness of the risk of a false alarm increased unjustifiably after the Blue-White Alert. Nonetheless, this was a counter-risk that should not have been ignored in a situation assessment that discussed the risk of surprise. The challenge of the decision makers is to find the right balance by estimating the expected loss of each risk. In the situation that prevailed on the eve of the Yom Kippur War, estimating that the expected damage of the risk of a surprise attack was much greater than the risk of a false alarm was appropriate. In the end, this risk stood in the way of the decision makers**.**

The risk of the regular army's failure to contain the attack

The strategic risk that the regular army would have difficulty containing the attack until the arrival of reserve forces was not sufficiently established by the cabinet before the war. There is little evidence in prior discussions about this risk. The collapse of the regular army at the containment stage seems to have shocked the chief of staff and the defense minister, as well as the prime minister, who had trusted their judgment. On this matter, the military leadership erred in their concept, which was no less erroneous than the intelligence concept.[45]

The expectation that the regular army would contain the attack was unfounded, due to the extreme force ratios at the front lines, which were detrimental to the IDF (one division versus the Egyptian army and one division versus the Syrian army), especially when the two enemy armies were deployed at emergency positions on the front lines. For example, the Dovecote Plan was not built for containing a large Egyptian offensive order of battle. The mission (according to Dovecote) of preventing the enemy any achievement in the early stage of the war was not compatible with the balance of power on the ground and the risks posed to the regular army. A different risk management could have actually led to the early evacuation of the *maoz* outposts. In the end, the risk materialized; either it was not managed, or its management had failed.

45 Shmuel Even, "The Conceptual Failures of Advanced Warning in the Yom Kippur War and What Can Be Learned from Them?" *Maarchot* no. 388 (November 1994).

The risk involved in a preemptive strike

The political echelon decided not to take the risk of a preemptive strike in the hours before the outbreak of the Yom Kippur War, lest Israel be seen as the aggressor and bear the consequences. From the perspective of the chief of staff, the risk that the political echelon would prevent him from carrying out actions that he saw as essential for the campaign had been realized. Unlike the situation in 1967—when it was decided to conduct a preemptive strike—the strategic depth in 1973 gave the political echelon the feeling that it had greater room to maneuver; thus it was decided not to take the risk of a preemptive strike. Defense Minister Moshe Dayan even insisted on not taking this risk in a meeting with the prime minister on the morning of October 6.

This case is an example of the tension between managing diplomatic and military risks. The decision by the political leadership to refrain from a preemptive air strike exacerbated the regular army's inferior position at the onset of the war and was a mistake, as Golda Meir understood immediately after the war began. We can speculate that if the political echelon had been aware of the strategic risk that the regular army would not contain the attack, it might have approved a preemptive air strike. It seems that the meetings with the prime minister lacked any mention of the cross risks, when avoiding one risk intensifies the other risk.

It should be noted that Henry Kissinger later conjectured that the decision not to carry out a preemptive air strike "was a reasonable judgment by Golda, in balancing between the image of Israeli aggression, if you had acted first, and the actual effectiveness that would have been achieved in the short time that remained."[46] However, Kissinger's conjecture regarding the effectiveness of an attack was not based on knowledge about the readiness of the air force and the amount of time that Israel had to prepare (from the morning hours). In summary, it seems that not taking the risk of a preemptive strike was a grave error by Israel's cabinet.

Conclusion

Risk management supports carrying out operative actions, even in situations in which the likelihood of the risk is not high, but the potential damage is great. One of the advantages of risk management is having a high level of

46 Oren, "Henry Kissinger: You Know We Saved You in '73, Right?"

awareness of the possible risks and being prepared for them, which should shorten the response time and even reduce the cost of an error.

The IDF and the other defense forces must map out the risks that stand in the way of achieving their objectives (including cross risks) according to different scenarios and to find ways to lower the risks, in cooperation with the various defense forces as well as with the political echelon, the National Security Council and the relevant government ministries. To do so, they must maintain a dialogue with the political echelon regarding operational plans, especially on situations where a political decision will be necessary.

It is important to emphasize that military and diplomatic risks at the strategic level should be managed together, as strategic military objectives are not separate from diplomatic goals. The military leadership must be aware of the constraints that the political echelon may dictate and the level of maneuvering room that it may have in different circumstances. This applies between wars, prior to war, and during war.

National Cyber Security in Israel

Yigal Unna

The challenges that the State of Israel faces in the field of cyber technology are affected by sweeping international social, cultural, and technological processes, far more than in other fields. We can identify two challenges or trends that influence cyberspace and are also shaped by it. The first trend—a leading global development—is the challenge of data. Information is the most significant resource of the past fifteen years and seemingly of the coming decades. The main issues relating to this challenge are how to transfer, move, store, and manage data, and how to maximize its benefit. Fifteen years ago, the world's biggest companies were those considered to have the highest value: energy, gas, and oil companies; today, they are information companies. The race for power through information and its control is expected to continue and even intensify in the future.

The second trend is the technological challenge or the "internet of everything," which—beyond the "Internet of Things—is connected to living human tissues for the purpose of monitoring and healing diseases and more. Israel is handling this challenge relatively well compared to the international arena. Israel could still invest more in the field, however, as formulated by the new Technological Intelligence Systems Initiative, pursuant to a directive by the Prime Minister, for identifying the main technologies that Israel should focus on in the near future, namely artificial intelligence, quantum computing, and other data technologies. This is in order to better prepare for the future as a national economic and social power.

Yigal Unna is the director general of the Israel National Cyber Directorate. This article is based on his speech given on October 24, 2018 at the conference held by INSS in cooperation with the Academic Center of Law and Science in Hod HaSharon to commemorate the publishing of the memorandum "Regulation in Cyberspace," by Prof. Col. (res.) Gabi Siboni and Ido Sivan-Sevilla.

The definitions of the terms "cyber," "cyber warfare," and "cyberspace" are constantly changing and being updated. The Israel National Cyber Directorate in the Prime Minister's Office works according to a broad definition that will always remain relevant in order to ensure that Israel has the broadest possible protection against all threats to information and communications technologies (ICTs) as well as additional threat profiles. In this respect, it is worth noting the series of state-level attacks that have taken place in recent years, such as the ongoing series of various attacks on Ukraine since 2014. None of these attacks has led to the collapse of the Ukrainian State, but they have completely disrupted its economy and undermined the public's confidence in the government and its ability to govern.

An assessment of the development of cyberspace and cyberattacks shows that in the beginning, these attacks were aimed at espionage and obtaining information and that they are taking place at greater volume and intensity. Over time it has become clear that by penetrating a computer system, it is possible not only to extract information from it, use it to disrupt critical processes, and even cause physical harm and death, but also to cause psychological harm and have a negative impact—again, all via cyber technology; i.e., by penetrating or breaking into an information system without permission and gaining access to it.

A recent example of psychological harm can be found in the attempts to disrupt the US elections in 2016 which, according to US claims, were under cyberattack. This incident clearly indicates the psychological impact that a cyberattack can have and its success in shaking up an entire election. Additional examples include penetrating the private email accounts of American senators and of a senior official in the US administration, not for the purpose of espionage or inflicting damage, but rather for collecting material that could be leaked at the right time and place in order to cause chaos and undermine the American public's confidence in its democratic and political system.

A well-known example of a psychological attack in the economic sphere occurred two weeks after the terrorist attack at the Boston Marathon in 2013. A tweet was posted on the Twitter account of the Associated Press, stating "Explosion at the White House, President Obama injured." The incident immediately affected the US stock market. In this case, however, the attacker was not sophisticated enough, as it took the news agency only seven minutes

to understand that someone had penetrated its computer system by simply guessing a password, which is known in the professional jargon as a "brute force" attack. In this case, the attacker stopped at the Twitter post and thus the damage was relatively limited. The most astonishing thing about the incident was that four Syrian hackers who belonged to the Syrian Electronic Army were discovered to be behind the breach. Their attack was an expression of the tension that existed between the US administration led by President Obama, and Syria, regarding the latter's use of chemical weapons.

The main insight from this incident is that four people (in this case, Syrian) lacking the capabilities of a superpower, demonstrated the potential to cause economic damage to the leading global superpower. This was not a penetration of the stock market's computers or of the American banking system; rather it was an attack that had a psychological impact. Thus, when characterizing the type of critical infrastructure that should be protected and the means of protection, public confidence should also be seen as a type of critical infrastructure needing protection. In this regard, it should always be assessed what the adversary, whoever it is, could do, via cyberattacks and by penetrating computer systems and computer networks, in order to undermine public confidence.

The asymmetry between these kinds of adversaries and states is sometimes to the detriment of the state, which is much more digital, far more dependent on advanced systems, and possesses critical computer-based infrastructure. Stateless terrorist organizations that have cyber capabilities—such as ISIS and Hamas—have an asymmetric advantage as they do not have critical infrastructure, a financial system, or even a public whose confidence must be maintained so that they can govern. Public confidence can be undermined by harming the financial, political, or democratic system. Nothing needs to actually collapse in these systems; rather, the feeling that something bad is going to happen to them is enough. This problem is even more complex in the cyber age, as the attack surface is expanding. These scenarios keep the National Cyber Directorate up at night.

Additional threat profiles that should be taken into account relate to the spread of superpower attack tools. The best example of this occurred in May 2017 when North Korea obtained a cyber tool attributed to the United States (Eternal Blue), which was leaked out of the labs of the National Security Agency and then used in a worldwide ransomware attack. The United States

was itself attacked, as was the United Kingdom. An official British report on the attack indicated that 139 urgent surgeries in the British health system had to be postponed as a result and damage was estimated at £2.5 billion. Unlike nuclear weapons, which so far have fallen into the hands of terrorists only in Hollywood movies, the leakage of superpower cyberattack tools has already occurred in reality.

As for cyberspace, all the players have capabilities, if only due to the nature of the cyberspace tools: they are made up of computer codes, which, once launched, are not usually destroyed and thus can easily be reused as a "cybernetic warhead," much more than a kinetic warhead that did not explode—provided that the weapon was not obtained first by leaking it from its production lab, as in the American case. Hence, Israel is exposed to the use of superpower tools against it.

Other threat profiles, beyond the scope of this paper, are threats to the supply chain and its defense, as well as cybercrime. It should be noted that the distinction between cybercrime and cyber threats to national security is becoming blurred as more criminal groups work for foreign governmental and military bodies. All these trends and threat profiles demand awareness and all possible means of action in order to protect against them.

Israel was one of the first countries to identify these trends and threats. As early as 2002, protection of computer and information infrastructure was defined as critical and vital, and the task was assigned to the Shin Bet. A decade later, the State understood that more was necessary, and in 2012, on the initiative of Prime Minister Netanyahu, a national directorate was created to address strategy and all aspects of national cyber issues. Two years later, the need arose for a separate operative authority that would handle cyber events in the civilian sphere, and in 2016 the National Cyber Security Authority was established. The State very quickly understood that these two support units should not operate separately or even competitively, and in January 2018, they were merged into a single directorate—the National Cyber Directorate—whose first and foremost task is protecting Israeli cyberspace.

The National Cyber Directorate's second task, which is closely connected to the first, is furthering Israeli leadership in the global cyber arena. The State of Israel has created a unique cyber ecosystem that incorporates the government, academia, and industry, based on the conception that investment in human capital and industry are necessary for maintaining high-quality

protection and superiority over time. Israel and its National Cyber Directorate have established six academic research centers in partnership with various universities and have developed a model for advancing and investing in the Israeli cyber industry, which contributes to the state, to society, and to the economy, and thus to national resilience in general and cyber security in particular.

The position of Israel's cyber industry is manifested in the annual survey of 500 leading companies in the field known as the Cyber Security Ventures. It covers 354 American companies, followed by 42 Israeli companies. The United Kingdom is ranked third, with half as many companies as Israel, followed by a long list of companies from various other countries. According to the survey, there are another 40 or so Israeli companies that are located in Israel but registered in the United States for tax and trade considerations. Thus, the real numbers are about 310 American companies versus 80 Israeli companies; i.e., four times as many, whereas the ratio between the economies and populations of the two countries is much higher.

Israel has succeeded in developing a cyber security strategy that includes three layers: durability, resilience, and national defense. The durability layer is akin to hygiene, a kind of hand washing before eating in order to stay healthy. Investing in this layer is cheaper than investing in the next layers. Regulation is aimed mainly at this layer. The resilience layer is based on the assumption that attacks will occur, and in order to recover from them as quickly as possible and with as little damage as possible, we should prepare accordingly. The third layer, in which the National Cyber Directorate is not at all involved, handles and thwarts attackers. The Israel Defense Forces and the other defense institutions are the ones who deal with this, although the National Cyber Directorate is a partner in the effort by assisting, guiding, and providing information.

This is the strategy underlying the National Cyber Directorate. It operates a national emergency center for handling cyber events, which operates twenty-four hours a day, every day of the year. This is the national CERT (Computer Emergency Response Team) facility, which is located at Cyberspark in Beersheba. Any citizen and organization that suspects that it has been cyber attacked can contact the center and receive assistance and guidance.

Israel has many independent cyber capabilities on the level of a superpower. Nonetheless, international cooperation is still a vital need for Israel. Thus,

the Cyber Directorate works in cooperation with over seventy emergency centers around the world to handle cyber events. It is also a member of and takes part in international cyber forums and is a partner in the assistance programs of various organizations such as the World Bank, the Development Bank of Latin America, and others. Cyber cooperation aims first of all to address operative and defensive needs. Those who attack Israel, such as Iran, do not do so directly but instead via other countries, most of them friendly toward Israel. The more connections Israel has and the more it creates a shared language with these countries, the easier, better, and more effective the work of defense and deterrence will become.

Cyber security in civil aviation, in which the National Cyber Directorate leads and has invested considerable effort, is a good example of international cooperation between forces. It aims to address phenomena connected to the modernization of aviation, which in itself is a welcome development. Passenger aircraft such as the Dreamliner and the Airbus 380 are high tech. Today, flight plans for the newest aircraft, as well as for older ones, are received via tablet computers and not in writing as in the past. This is only one example of possible cyberattack avenues. In order to be prepared for such attacks, the Directorate facilitated the establishment of a consortium of Israeli companies, led by Israel Aerospace Industries and including companies such as Check Point and El Al, to develop and provide solutions in this area.

The National Cyber Directorate's focus on cyber security in civil aviation combines its two main tasks: protecting Israeli cyberspace—in this case, civil aviation and airports in general, which are defined as critical infrastructure—and furthering Israel's global cyber leadership. The combination of aviation, security, and cyber considerations directly connects with Israel's strength and its comparative advantage.

Without ignoring the current public discourse on protecting the democratic process, the National Cyber Directorate focuses on a cyber-technological orientation and carries out a comprehensive systemic assessment well before Election Day. The directorate works in cooperation with the Central Elections Committee on the vote-counting process, which is just a tiny piece of the entire process. In addition, the directorate provides the entire economy, the media, the polling institutes, and additional organizations through which public opinion can be influenced, with recommendations for protection

in cyberspace in order to ensure that Israel's democratic process is free of foreign influences and unwanted interference in various cyber scenarios.

In democracy, there is a separation of powers; in cyber, it is customary to talk about a separation of networks. The National Cyber Directorate provides guidance on critical infrastructure that is under the government's responsibility but does not offer guidance to the other government branches, such as the legislative or judicial branches. It would not be appropriate to do so in a democracy, and the Cyber Directorate takes this very seriously. In this way, the government (via the Cyber Directorate) refrains from instructing the Central Elections Committee, the Knesset, or the State Comptroller on cyber issues, and instead works according to the model of "voluntary guidance;" i.e., voluntary cooperation in sharing knowledge, which works well. These bodies decide independently what they do in cyberspace and in terms of their cyber security. The National Cyber Directorate provides them with the knowledge, intelligence, and comprehensive support needed in order to succeed, each in its field and in accordance with its area of responsibility.

The National Cyber Directorate is currently working on developing a national defense architecture through a multi-year, advanced technological perspective, at the end of which it will be possible to share as much information as possible with partners in Israeli cyberspace and succeed in the early discovery, identification, and elimination of cyberattacks. The cyber law that the National Cyber Directorate is promoting is a critical tool for the success of Israel's cyber security. To this end, the Cyber Directorate also supports the international cyber coalition with senior officials in many countries that are friendly toward Israel.

The guiding principle of the National Cyber Directorate is collaboration, creation of partnerships, and expanding the circle of defense partners, as no single body—no agency, government ministry, or state—can cope alone with the enormous challenges which have been briefly reviewed here. United we stand strong; divided—we fall.

Cyber, Intelligence, and Security

Call for Papers

The Institute for National Security Studies (INSS) at Tel Aviv University invites submission of articles for ***Cyber, Intelligence, and Security***, a new peer-reviewed journal, published three times a year in English and Hebrew. The journal is edited by Gabi Siboni, head of the Cyber Security Program and the Military and Strategic Affairs Program at INSS.

Articles may relate to the following issues:

- Global policy and strategy on cyber issues
- Cyberspace regulation
- National cybersecurity resilience
- Critical infrastructure cyber defense
- Cyberspace force buildup
- Ethical and legal aspects of cyberspace
- Cyberspace technologies
- Military cyber operations and warfare
- Military and cyber strategic thinking
- Intelligence, information sharing, and public-private partnership (PPP)
- Cyberspace deterrence
- Cybersecurity threats and risk-analysis methodologies
- Cyber incident analysis and lessons learned
- Techniques, tactics, and procedures (TTPs)

Articles submitted for consideration should not exceed 6,000 words (including citations and footnotes), and should include an abstract of up to 120 words and up to ten keywords. Articles should be sent to:

Hadas Klein
Coordinator, ***Cyber, Intelligence, and Security***
Tel: +972-3-6400400 / ext. 488
Cell: +972-54-4510411
hadask@inss.org.il

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
TEL AVIV UNIVERSITY אוניברסיטת תל אביב

The Institute for National Security Studies – Cyber Security Program
40, Haim Levanon St, POB 39950, Ramat Aviv, Tel Aviv 61398 | Tel: +972-3-6400400 | Fax: +972-3-7447588