Cyber, Intelligence, and Security

Volume 4 | No. 1 | March 2020

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

Cyber, Intelligence, and Security

Volume 4 | No. 1 | March 2020

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 twice 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, Tel Aviv University Graphic Design Studio
Printing: Digiprint Zahav Ltd., Tel Aviv

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)

The Secret War of Cyber Influence Operations and How to Identify Them

David Tayouri

Social media is an effective way of influencing human society and behavior and shaping public opinion. Cyber influence operation means using cyber tools and methods in order to manipulate public opinion. Today, many countries use cyberspace, and specifically social media, to manage cyber influence operations as part of holistic information warfare. Most of these operations are done covertly and, therefore, identifying them is challenging; moreover, it is not an easy task to differentiate between legitimate or malicious influence operations. This paper will describe cyber influence operations, the potential damages that they could incur, and how they are conducted. Furthermore, the paper will analyze the challenges of identifying such operations and will detail several indicative parameters with which cyber influence operations can be identified.

Keywords: Cyber influence, influence operation, social media, social engineering, cyberwarfare

Introduction

The digital era has changed the way we communicate. Nowadays, relationships and conversations between people take place through the web and digital communication. Using social media—such as Facebook and Instagram—and social applications—such as WhatsApp and Telegram—we can keep in touch with our friends and family; share posts, messages, pictures, and

David Tayouri is deputy director of Engineering, the National and Aviation Cyber Programs Directorate, Cyber Division, ELTA Systems Ltd. at the Israel Aerospace Industries (IAI). The author would like to thank Mr. Aaron (Ronnie) Eilat and Mr. Mark Ellins for reviewing this article and for their thoughtful comments.

videos; share our experiences with each other, be updated on our friends' statuses, and read their posts.

Social media, which is vastly used by many people around the world, is also an effective way of influencing human society and behavior and shaping public opinion. By sharing a post, tweeting an opinion, contributing a discussion in a forum, and sharing a sentimental or political picture, we can influence others and sometimes convince them with our opinion. Now imagine that you could participate in hundreds and thousands of digital conversations—you would have the chance of influencing large communities.

Using cyber tools and methods to manipulate public opinion is called a cyber influence operation. These operations may have different purposes: influencing psychologically, hurting morale, influencing public awareness, instilling a lack of control and the inability to protect the normative way of life, and more. Since these operations may cause (psychological) damage, they are also known as disinformation cyberattacks.

Today, many countries use cyberspace, and specifically social media, to manage cyber influence operations as part of holistic information warfare. Most of these operations are done covertly; in cases where the operation is revealed, it would be difficult to prove who stands behind them. Influence operations can be aimed at the general public with generic statements or can be directed at a specific audience with targeted messages in order to achieve more effective influence and to control their responses. An example of a response could be voting for a specific candidate or party in an election as was witnessed during the US presidential elections in 2016.

Identifying cyber influence operations is challenging. It is not an easy task to identify influence and specifically to differentiate between legitimate and malicious influence operations. Promoting a product or a decent idea is legitimate, even as an influence operation. Incitement, promotion of radical or violent acts, and intervention in democratic elections are examples in which malicious influence operations could be used. Nevertheless, it is important for governments, through defense organizations and law enforcement agencies, to identify malicious influence operations, in order to prevent them or, at least, to reduce their damages. Today, there is no systematic way of identifying cyber influence operations and differentiating between legitimate and malicious influence operations.

The following sections describe cyber influence operations and their potential damages, how cyber influence operations are conducted, and which tactics they use. The challenges of identifying cyber influence operations are analyzed and several indicative parameters with which cyber influence operations can be identified are detailed. The final section presents a case study of a cyber influence operation.

Cyber Influence Operations

A cyber influence operation can be defined as focused efforts to understand and engage key audiences in order to create, strengthen, or preserve conditions favorable for advancing interests, policies, and objectives, through the use of coordinated programs, plans, themes, messages, and products.[1] To put it simply, cyber influence operations create communications and interactions with the aim of influencing target audiences in order to change their opinion and/or behavior. If the purpose is controlling the responses of the group members, this is called *perception management*.

A theory similar to perception management, studied mainly in Russia, is *reflexive control*.[2] Reflexive control is defined as a means of conveying to a partner or an opponent specially prepared information to incline him/her to voluntarily make the predetermined decision desired by the initiator of the action. A "reflex" involves the specific process of imitating the opponent's reasoning or the opponent's possible behavior, thereby causing one to make an unfavorable decision. In order to influence a state's information resources, reflexive control measures can be used against its decision-making processes. This aim is best accomplished by formulating certain information or disinformation designed to affect a specific information resource. If successfully achieved, reflexive control over the opponent makes it possible to influence their plans, their view of the situation, and how they would fight. In other words, one side can impose its will on the other and cause them to make a decision inapposite to a given situation.

A close term to cyber influence in the military context is *influencing maneuver*, which is the process of using (cyber) operations to get inside an enemy's decision cycle or even forcing that decision cycle to direct or

1 Eric V. Larson, and others, *Understanding Commanders' Information Needs for Influence Operations* (Santa Monica: Rand Corporation, 2009).

2 Timothy L. Thomas, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies* 17, no. 2 (2004): 237–256.

indirect actions. It is a broad form of maneuvering intended to gain and maintain information superiority and dominance and to maintain freedom of maneuver in cyberspace.[3] Influencing maneuver can be used in direct or indirect operations. A direct example of influencing maneuver could include actions such as compromising command and control systems and manipulating data subtly in order to degrade the confidence that a commander has in the systems and to slow down decision cycles. Indirect actions might include feeding compromised and manipulated data to the media in order to force a desirable reaction from an enemy. In this article we will focus on indirect actions.

Influence operations have emerged as a major concern worldwide. They come under different names and in various flavors—fake news, disinformation, political astroturfing, information attacks, and so forth. They may arrive as a component of hybrid warfare—in combination with traditional cyberattacks (use of malware)—and with conventional military action or covert kinetic attacks.[4]

An influence operation may have different purposes and potential effects/damages. In times of peace, the purpose of influence operations can be promoting desired ideas or leading groups to preferred directions. An example is a political party that manages a campaign to convince its constituents to vote for the party. If the same operation is performed by a foreign country, this, of course, will be deemed as intervening in a sovereign country's domestic affairs. Foreign intervention could damage the trust that the citizens have in their government, because they cannot be sure that the same government would be elected without the foreign intervention.

In times of conflict or war, the purpose of influence operations can be to create anti-government discussions, turn public opinion against government actions (e.g., actions of war), hurt public morale (e.g., creating a feeling of insecurity because of government actions), and so forth, all with the aim of giving a sense that the government has no control or ability to protect the

3 Scott D. Applegate, "The Principle of Maneuver in Cyber Operations," *2012 4th International Conference on Cyber Conflict (CYCON 2012),* (Tallinin: NATO CCD COE Publications, 2012), https://www.ccdcoe.org/publications/2012proceedings/3_3_Applegate_ThePrincipleOfManeuverInCyberOperations.pdf.

4 "Army Researchers Join International Team to Understand, Defeat 'Disinformation' Cyberattacks," *ARL Public Affairs*, December 5, 2017, https://www.army.mil/article/197316/army_researchers_join_international_team_to_understand_defeat_disinformation_cyberattacks.

normative way of life, which eventually may weaken the country's army in the battlefield.

Influence operations can be aimed at the general public or at a specific audience, which can be targeted using online databases or social networks. Influence operations aimed at the general public will include generic statements, which will have a minimal influence at the micro level on individuals but can still reach the desired effect at the macro level. Influence operations aimed at specific audiences will use statements tailored to that audience in order to be more effective.

How Cyber Influence Operations Are Conducted

The first step in conducting an effective cyber influence operation is defining the goal of either building one—by promoting a subject, strengthening it, improving public opinion of it—or harming one by attacking the opponents, weakening the adversaries, and creating negative public opinion. The second step is determining the coverage and audience: a wide audience, targeted groups, or a small group of influencers; radical or consensus groups; and which gender, age, race, religion, and so forth will best serve the goal. The third step is selecting the social networks and forums in which the influence operation will be conducted and determining the interaction between the selected medium and other intermediaries. The fourth step is determining the tools for spreading the messages: fake profiles, bots, or trolls. Fake profiles may have a better reputation, but they need manual intervention. Bots can be programmed to reply automatically to defined content, but they may be easily identified as bots. Trolls are used when using aggressive negative content, usually when the goal is to attack opponents. The last step is defining the appropriate messages and publishing them intensively, according to the defined goal and audience. Figure 1 below depicts the steps of operating cyber influence operations.

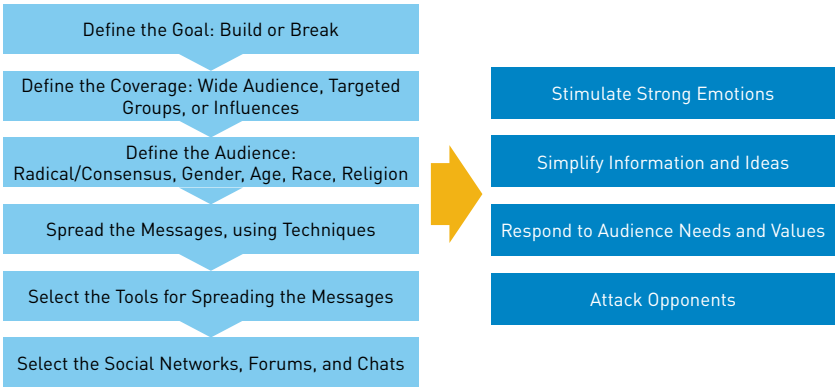

Figure 1. The Steps of Operating Cyber Influence Operations

Propaganda has always been a common way of influencing people. Modern propaganda is very effective since it relies on the digital and social media. It can easily reach many people or selected groups and uses a large number of posts to achieve its goal. Cyber influence operations may use the same techniques as propaganda to successfully influence people,[5] including:

- **Stimulating strong emotions** such as fear, hope, anger, frustration, and sympathy in order to direct audiences toward the desired goal. In the deepest sense, it is a mind game—the skillful influence operator exploits people's fears and prejudices. Successful influence operators understand how to psychologically tailor messages to people's emotions in order to create a sense of excitement and arousal for the purpose of suppressing critical thinking and exasperating emotions instead.
- **Simplifying information and ideas** by using accurate and truthful information, half-truths, opinions, lies, and falsehoods. A successful influence operation tells simple stories that are familiar and trusted, often using metaphors, imagery, and repetition to make them seem natural or "true." Oversimplification is effective when catchy and memorable short phrases become a substitute for critical thinking. Oversimplifying information does not contribute to knowledge or understanding; rather because people naturally seek to reduce complexity, this technique of influence operation can be effective.

5 "Recognizing Propaganda," *Mind Over Media*, https://propaganda.mediaeducationlab.com/techniques.

- **Responding to audience needs and values** by conveying messages, themes, and language that appeal directly—and many times exclusively—to specific and distinct groups within a population. A cyber influence operator may appeal to people using their racial or ethnic identities, hobbies, favorite celebrities, beliefs and values, or even personal aspirations and hopes for the future. Using different social media profiles, this task becomes easier and more effective, since each profile can be adjusted to the target audience in order to achieve the best influence result.

  Sometimes, universal deepest human values—the need to love and be loved, to feel a sense of belonging and a sense of place—are activated. By creating messages that appeal directly to the needs, hopes, and fears of specific groups, an influence operation becomes personal and relevant. When messages are personally relevant, people pay attention and absorb key information and ideas.
- **Attacking opponents** by serving as a form of political and social warfare to identify and vilify opponents. It can call into question the legitimacy, credibility, accuracy, and even the character of one's opponents and their ideas. Because people are naturally attracted to conflict, an influence operation can make strategic use of controversy to get attention. Attacking opponents also encourages "either-or" or "us-them" thinking, which suppresses the consideration of more complex information and ideas. Furthermore, influence operations can also be used to discredit individuals, destroy their reputation, exclude specific groups of people, incite hatred, or cultivate indifference.

Challenges of Identifying Cyber Influence Operations

In order to identify cyber influence operations, first we should identify cyber or social influence. Therefore, one of the basic challenges is to define what social influence is and how to measure it within a network. Social influence is defined as "consciously or subconsciously persuading others from your thoughts, beliefs or actions."[6] There are three categories in defining social influence: **actors**, **interactions**, and **networks**.

To achieve the largest possible audience, in many cases, cyber operators approach influencers. There are different indicators for identifying the potential

6 D.M. Kahan, "Social Influence, Social Meaning and Deterrence," *Virginia Law Review* 83, no. 2 (1997): 349–395.

of an **influential actor** (i.e., influencer): active minds, trendsetters, social presence and impact, social activity, charisma, expertise, authority, number of followers/friends, and more. An actor has influence in a network if the message is shared outside his/her own network; the message is shared by others in the network; the actor has a large number of contacts; the actors causes others to read a message; and the speed in which a message is shared/used within a network is high.

The **influential interaction** can be measured with different indicators. Dutch researchers have found that the influence of an interaction largely depends upon the following: the number of times a message has been shared; the types of reactions that a message causes; the number of times a message has been quoted; number of readers/listeners reached; and if the message brings a large group of unique visitors.[7]

One of the commonly used and influential sites for interaction in cyberspace are weblogs. The following is different criteria for testing influence within the context of weblogs:[8]

- Network centrality score—measures the reputation of an individual. Is he/she a central person in a network or just someone with a limited number of contacts?
- Hyperlink authority score—measures the number of links to a blog as a criterion for influence.
- Site traffic score—measures the number of website visitors.
- Community activity score—relates to the number of comments that a blog evokes.

Similarly, additional studies have associated other indicators with **influential social networks**, including the social distance between two actors, reciprocity, multiplexity, size of the network, density, connectivity, centrality, emotional value, group cohesion, and clustering.

7 Wouter Vollenbroek, Sjoerd de Vries, Efthymios Constantinides, and Piet Kommers, "Identification of Influence in Social Media Communities," *International Journal of Web Based Communities* 10, no. 3 (2014): 280–297.

8 Dave Karpf, "Measuring Influence in the Political Blogosphere: Who's Winning and How Can We Tell?" *Politics and Technology Review* (2008): 33–41, http://www.the4dgroup.com/BAI/articles/PoliTechArticle.pdf.

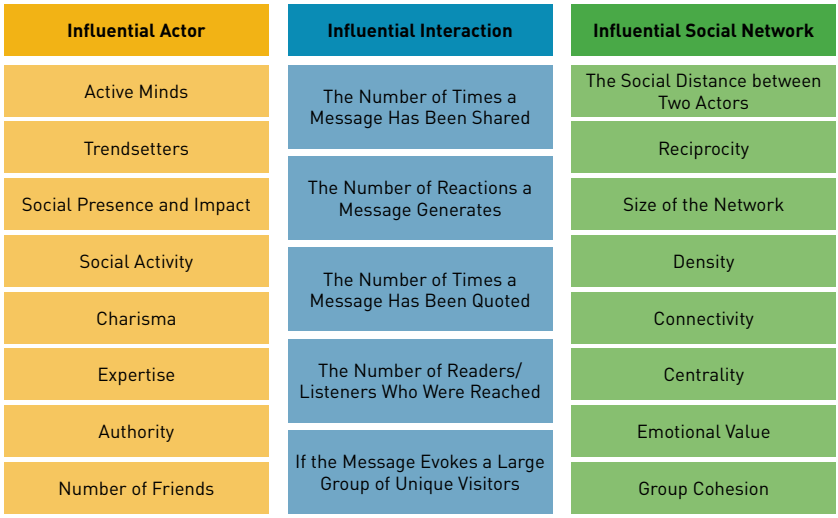

Figure 2. Social Influence Indicators

These well-defined indicators can be used to find influential actors, interactions, and networks, which, in turn, can help us to better identify social influence. Figure 2 above summarizes the social influence indicators.

After identifying social influence, the next challenge is differentiating between legitimate and malicious influence operations. Sometimes the legitimacy of an influence operation is in the eyes of the beholder. Most people will agree that incitement and promotion of radical or violent acts constitute malicious influence operations, and that promoting a decent idea is usually legitimate freedom of speech. But what about political ideas or statements that are expressed against a country's leadership? Well, it may depend on the country's values and regime. Let's take a democratic regime, in which a person can criticize anything and anyone, including the country's leader. If this was done by an army of bots, which were programmed to automatically spread statements against the leading party, the legitimacy of the statements would not be very clear, especially when using bots is prohibited by most countries. If this army was managed by a foreign actor, it would probably be considered as foreign intervention in a sovereign's democracy.

Sometimes, to influence effectively, fake news is used. For instance, Saudi Arabia and the UAE worked to sway American public opinion and other Arab countries against Qatar through online and social media campaigns, by accusing Qatar of supporting terrorism and destabilizing the region, a

charge Doha rejected, and which eventually appeared to be false. The result of this campaign was that during June 2017, Saudi Arabia and the UAE led other Arab countries to cut diplomatic relations with Qatar.[9] We can agree that using fake news is not legitimate and may indicate a malicious influence operation, but the real challenge is in identifying it. Mostly, fake news is published together with other authentic news, making it difficult to spot. Identifying fake pictures is also challenging, with all the advanced picture editing tools available today. The situation becomes complicated when a particular post may include some facts, some bogus facts, and some commentary that naturally is subjective, depending on the writer's values and beliefs. In social media, such a post receives comments from others, reflecting their opinions and perspectives, which make it even harder to identify the false elements.

Another challenge in identifying cyber influence operations is that the process should be done in near real time. In social media, news spreads very fast; therefore sometimes until a fact is revealed as false, the damage has already been done and influence operation goals have been promoted. For example, spreading fake or semi-fake news about a candidate a few days before the elections may change the results.

After a cyber influence operation is identified, we usually want to know who stands behind it and collect evidence to prove it. The challenge here is that the people or the group behind the influence operations usually hide their tracks and do not reveal their true identity, by using bots and fake profiles in social media, and by concealing their communication parameters (such as their IP) with the use of dedicated browsers for anonymous browsing or by using proxy servers.

Indicative Parameters for Identifying Cyber Influence Operations

To identify cyber influence operations, the published content—text, pictures, and videos—in the various social networks should be monitored and analyzed using operations research and advanced algorithms, taking into account many

9 Josh Wood, "How a Diplomatic Crisis among Gulf Nations Led to a Fake News Campaign in the United States," *PRI*, July 24, 2018, https://www.pri.org/stories/2018-07-24/how-diplomatic-crisis-among-gulf-nations-led-fake-news-campaign-united-states.

content- and communication-oriented parameters. The following indicative parameters may help identify a cyber influence operation:

- **Use of avatars, bots, and trolls**—a good influence operation will hide its operators in order to achieve the most effective results. There are several ways of anonymizing the influence operation, but two of the most used tools are avatars and bots. Avatars are virtual identities in social media, which hide their operator's true identity. Bots are small agents, which are programmed to automatically respond to specific posts or publish automatic posts to promote their programmed idea/product. Many tactics can be used to identify bots. Two researchers have found a number of traits to spot a bot, such as having a sleepless account, engaging in high-volume retweeting, replying to content that contains certain keywords, using stolen profile images, having unreal profile names, showing significant gaps in the account activity, and more.[10]
- **Publishing of posts and news by factors outside of the country**—it is a legitimate action when people try to convince other people and promote their own ideas or beliefs, as long as this is done in their own country or done from another country but without hiding their identity. But if someone from another country impersonates a local citizen, it is suspicious and should be investigated. A good example of this is trying to influence results of elections in another country. It should be mentioned that it is not an easy task to discover the real source of published content. VPS (Virtual Private Server) based in the target country may be used to mask the location of the individuals involved. Email accounts based in the target country and linked to fake or stolen identities may be used to back the online identities. These identities may also be used to launder payments through PayPal and cryptocurrency accounts.
- **Publishing of fake news**—this is one of the more efficient methods of influencing public opinion as witnessed in the case of the US and French elections. Researchers from Stanford found that 62 percent of American adults get their news on social media, that the most popular fake news stories were widely shared on Facebook, and that many people exposed

10 Bill Fitzgerald and Kris Shaffer, "Spot a Bot: Identifying Automation and Disinformation on Social Media," *Data for Democracy*, June 5, 2017, https://medium.com/data-for-democracy/spot-a-bot-identifying-automation-and-disinformation-on-social-media-2966ad93a203.

to fake news stories report that they believe them.[11] This means that fake news disseminated on social media is a good tactic for influence operations and, therefore, a good indicator for identifying this kind of operation.

- **Publishing a large number of items on a specific subject**—to reach as many people as possible and in order to increase the influence, numerous items about the subject of influence need to be published. For instance, if one country plans a military action against another country, the latter could publish a large number of posts and tweets against the action, addressing the possible damages to the economy, exaggerating the number of casualties, the harm to human rights, and so on.
- **A sudden change of public opinion**—when looking at specific groups on social media and internet forums, changes in public opinion over a short period of time may indicate foreign intervention, because changes in opinions tend to be gradual. For example, in an election, if a leading candidate suddenly loses the lead in a day or two, this could be an indication of external intervention.
- **Publishing radically negative phrases**—to achieve a fast and effective change of public opinion in relevant groups or forums, extremely negative phrases may be used and may indicate an incitement operation. For instance, if a political group is vilified by calling into question their legitimacy and credibility by using extremely negative expressions, this should raise a red flag.

Figure 3 below depicts the indicative parameters for identifying cyber influence operations. A single parameter is not enough to indicate an influence operation, but a combination of several parameters could suggest that an influence operation is being conducted. In addition, the process can be automated by an algorithm that will combine all the indicators, although they may differ depending on the situation. The indicative parameters should be given different weight according to their context.

11 Hunt Allcott and Matthew Gentzkow, "Social Media and Fake News in the 2016 Election," *Journal of Economic Perspectives* 31, no. 2 (Spring 2017): 211–236, https://web.stanford.edu/~gentzkow/research/fakenews.pdf.

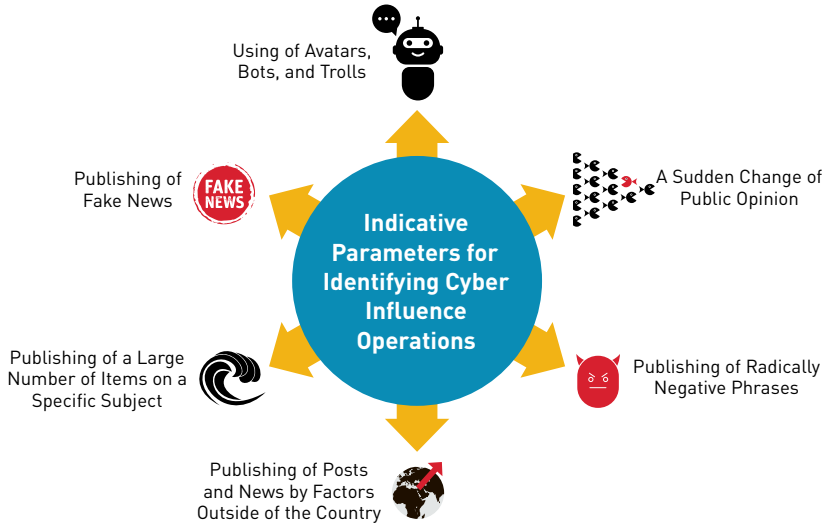

Figure 3. Indicative Parameters for Identifying Cyber Influence Operations

Case Study: Russian Intervention in the US Elections in 2016

Many cases of cyber influence operations were published over the last years, but one of the best known cases is the Russian intervention in the US elections in 2016. Analysis of this case shows that almost all the parameters mentioned in the previous section could be relevant for identifying the Russian influence operation in the 2016 US election:

- Russians publishing posts—On October 7, 2016, the Office of the Director of National Intelligence (ODNI) and the Department of Homeland Security (DHS) jointly stated that the US intelligence community was confident that the Russian government directed the hacking of emails in order to interfere with the US election process.[12] Two reports prepared for the Senate Intelligence Committee by independent researchers reveal that

12 "Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security," *Department of Homeland Security*, October 7, 2016, https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

Moscow's intelligence officials reached millions of social media users between 2013 and 2017.[13]

- Use of avatars and trolls—According to a ODNI report, the Russian campaign was multifaceted, including state-funded media, overt propaganda, and paid social media users or trolls.[14] Reports show the trolls used multiple websites to disseminate their narratives.[15] Facebook officials said that 470 fake accounts had been created since June 2015 and were used during the 2016 US election campaign by the Russian company Internet Research Agency (IRA), which is known for using "troll" accounts to post on social media and comment on news websites.[16]
- Fake news—In January 2017, the director of US National Intelligence testified that Russia also interfered in the elections by disseminating fake news promoted on social media.[17] In nearly 110 Facebook posts, including fake images of election machine error messages or ballots, the IRA targeted conservative users with false information about supposed widespread voter fraud aimed at helping Clinton win.[18]

13 Alex Ward, "4 Main Takeaways from New Reports on Russia's 2016 Election Interference," *Vox*, December 17, 2018, https://www.vox.com/world/2018/12/17/18144523/russia-senate-report-african-american-ira-clinton-instagram.

14 "Assessing Russian Activities and Intentions in Recent US Elections," *Office of the Director of National Intelligence*, January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

15 "Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security," *Department of Homeland Security*, October 7, 2016, https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

16 Scott Shane and Vindu Goel, "Fake Russian Facebook Accounts Bought $100,000 in Political Ads," *New York Times*, September 6, 2017, https://www.nytimes.com/2017/09/06/technology/facebook-russian-political-ads.html.

17 Ellen Nakashima, Karoun Demirjian, and Philip Rucker, "Top US Intelligence Official: Russia Meddled in Election by Hacking, Spreading of Propaganda," *Washington Post,* January 5, 2017, https://www.washingtonpost.com/world/national-security/top-us-cyber-officials-russia-poses-a-major-threat-to-the-countrys-infrastructure-and-networks/2017/01/05/36a60b42-d34c-11e6-9cb0-54ab630851e8_story.html.

18 "Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security," *Department of Homeland Security*, October 7, 2016, https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

- Publishing many items on the candidates—One of the fake news items about Secretary Clinton was shared 800,000 times.[19] Instagram saw an estimated 20 million users engage roughly 187 million times with IRA content related to the election, while Facebook had 76.5 million engagements that reached about 126 million people.[20]
- Many negative phrases about the candidates—According to the ODNI, Russia helped Trump's election chances by discrediting Secretary Clinton and publicly contrasting her as unfavorable.[21] When it appeared to Moscow that Secretary Clinton was likely to win the presidency, the Russian influence campaign focused more on undercutting Secretary Clinton's legitimacy and crippling her presidency from its start, including to impugn the fairness of the election. According to the Computational Propaganda Research Project, the Russian company IRA used many tactics to shape public opinion in the United States by spreading misinformation on social media platforms, exploiting social media platforms for foreign influence operations, and amplifying hate speech or harmful content through fake accounts or political bots.[22]

Other Case Studies

As mentioned above, the 2016 US election was neither the first nor the last known cyber influence operation. Following are a few other cyber influence operations:

- Pro-Russian hackers launched a series of cyberattacks over several days to disrupt the Ukrainian presidential election in May 2014 by releasing

19 Ellen Nakashima, Karoun Demirjian, and Philip Rucker, "Top US Intelligence Official: Russia Meddled in Election by Hacking, Spreading of Propaganda," *Washington Post,* January 5, 2017, https://www.washingtonpost.com/world/national-security/top-us-cyber-officials-russia-poses-a-major-threat-to-the-countrys-infrastructure-and-networks/2017/01/05/36a60b42-d34c-11e6-9cb0-54ab630851e8_story.html.

20 Alex Ward, "4 Main Takeaways from New Reports on Russia's 2016 Election Interference," *Vox*, December 17, 2018, https://www.vox.com/world/2018/12/17/18144523/russia-senate-report-african-american-ira-clinton-instagram.

21 Alex Ward, "4 Main Takeaways from New Reports on Russia's 2016 Election Interference," *Vox*, December 17, 2018, https://www.vox.com/world/2018/12/17/18144523/russia-senate-report-african-american-ira-clinton-instagram.

22 Philip N. Howard, Bharath Ganesh, and Dimitra Liotsiou, "The IRA, Social Media and Political Polarization in the United States, 2012–2018," Computational Propaganda Research Project, 2018, https://int.nyt.com/data/documenthelper/534-oxford-russia-internet-research-agency/c6588b4a7b940c551c38/optimized/full.pdf.

hacked emails, attempting to alter vote tallies, and delaying the final result with distributed denial-of-service (DDOS) attacks.[23]

- In December 2016, Ben Bradshaw, a member of the British Parliament, claimed that Russia had interfered in the Brexit (the exiting of the United Kingdom from the European Union) referendum campaign.[24]
- During the 2017 presidential election in France, automated accounts shared fake news about the election, and much of it came from sources that were exposed to Russian influence.[25] Russian influence was introduced into the French political discourse via content about international issues. This content was framed to undermine traditional media sources, minimize issues raised in opposition to Russian activities, or otherwise shift the focus and blame to other actors. The content served to mitigate criticism of Russia and create support for its political positions and, implicitly, the presidential candidates who espouse them.

Cyber influence operations may infect also the commercial space. Nike came under digital attack—a coordinated, operational campaign—after it rolled out the Colin Kaepernick campaign during September 2018.[26] Goals of this cyberattack included driving down the company's sales and share price. The following indicative parameters could be used to identity this operation:

- Use of avatars and bots—Certain groups were promoting a boycott against Nike by organizing echo chambers to mobilize tweets or deploying computer-generating traffic with bots. Inspection of the active users revealed that 426 out of 668 sampled users attacking Nike were avatars.
- Publishing many items against Nike—One of the coordinated influence campaigns had 300 users and generated about 2,133 tweets and retweets in a short time.

---

23 Mark Clayton, "Ukraine Election Narrowly Avoided 'Wanton Destruction' from Hackers," *Christian Science Monitor*, June 17, 2014, https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers.

24 Joe Watts, "Labour MP Claims It's Highly Probable' Russia Interfered with Brexit Referendum," *Independent*, December 13, 2016, https://www.independent.co.uk/news/uk/politics/russian-interference-brexit-highly-probable-referendum-hacking-putin-a7472706.html.

25 Pierre Haski, "Patterns of Disinformation in the 2017 French Presidential Election," *Bakamo*, 2017, https://www.bakamosocial.com/frenchelection/.

26 Jay Solomon and Aftan Snyder, "Lessons for Brands from the Anti-Nike-Kaepernick Social Effort," *PRNEWS*, February 22, 2019, https://www.prnewsonline.com/social+media-Nike-Kaepernick-APCO-bots-Twitter.

- Using many negative phrases—Users posted at least ten negative tweets or retweets during the campaign.
- A sudden change of public opinion—Nike's share price fell 3.2 percent the day after the campaign debuted.

Conclusion

Social media, which is vastly used by people around the world, is also an effective way of influencing social behavior and shaping public opinion. Cyber influence operation uses cyber tools and methods to manipulate public opinion. Today, many countries use cyberspace, particularly social media, to manage cyber influence operations as part of mostly covert holistic information warfare. When an influence operation is used to intervene in the internal affairs of another country, this may damage the trust that citizens have in their government. In addition, it may cause anti-government discussions, actions, protests, and harm public morale. Therefore, it is important for governments and defense organizations to identify cyber influence operations in order to prevent them or, at least, to reduce their negative influence. Although it is clear how cyber influence operations are conducted and which tactics they use, identifying them is not an easy task, since the influence operators use different masking tactics.

This paper introduced several indicative parameters for identifying cyber influence operations via published content, such as social media. Finding the parameters discussed here is challenging on its own, and each of them individually is not enough evidence of an influence campaign. Nevertheless, they may serve as a good starting point for a situation analysis, and their combined use simultaneously may provide a good indication that an influence operation is being conducted. The case study of the Russian influence operation in the 2016 US elections was a perfect example in which almost all the indicative parameters could be used to identify the operation, even at its earliest stages. This shows that the mentioned indicative parameters can be used systematically for detecting the next cyber influence operation. By constantly monitoring the relevant media, the mentioned practical approach enables early detection of the next cyber influence operation, even by non-expert analysts.

The cyber situation at the national level includes the state's critical national infrastructures, defense and government organizations, and so

forth. This cyber situation includes direct cyber events, including attempts of cyberattack, actual cyberattacks, and damage, but it should include also indirect cyber actions, such as cyber influence operations conducted by other countries. These operations should be considered covert wars and should be handled respectively, including allocating resources to identify and thwart them. Recommended further work includes determining additional indicative parameters, automating the influence operation identification process, and suggesting ways to defend against these operations.

Iran's Activity in Cyberspace: Identifying Patterns and Understanding the Strategy

Gabi Siboni, Léa Abramski, and Gal Sapir

This essay presents the evolving Iranian cyber activities with the purpose of identifying patterns that presumably form the cyber strategy applied by the regime to external and internal threats. The paper initially describes Iranian cyber operations, based on information released by the Islamic Republic and reports published by cybersecurity firms. The work then follows with an analysis of Iranian cyber activities. The article draws the characteristics and dynamics of Iran's cyber activities, both externally and internally, defensively and offensively. This survey highlights four common patterns identified in the research on Iranian cyber activities and is followed by an analysis of the main findings.

Keywords: Iran, cybersecurity, national cyber strategy, force buildup, internal and external threats, offensive and defensive activity

Introduction

Over the past decade, international observers may have minimized Iran's cyber capabilities as the relevant information documenting their existence is limited; however, perceptions of the Iranian threat have recently changed. At the 2019's edition of Cyber Week in Israel, Yigal Unna, the director-general of the Israel National Cyber Directorate affirmed that Iranians are among the five most active state actors in cyberspace. He stated that "the Iranians have

Prof. Gabi Siboni is the head of the Cyber Security program at INSS. Léa Abramski is a research intern at INSS. Gal Sapir is a research assistant in the Cyber Security Program at INSS.

been continuously active for a long time deploying broad attacks, including attacks to gather intelligence, influence operations, as well as attacks intended to cause harm and destruction to systems. Iran is one of the only countries to execute destructive attacks."[1] This recent shift in the way the Iranian threat is perceived among Western countries raises questions about the growing level of Iran's capabilities. It might be particularly noteworthy to identify the Iranian threat and to outline the characteristics of what appears to be Iran's national cyber strategy led against its adversaries. Indeed, experts have observed an intensification of Iranian activities in cyberspace, which is well documented by cybersecurity firms. According to a Microsoft survey published in March 2019, Iranian cyber groups have targeted thousands of people and more than 200 companies around the world during the past two years, causing significant damages estimated at hundreds of millions of dollars.[2]

Since the early twenty-first century, Iran has invested a significant portion of its budget in improving cyber capabilities. In the first three years of President Rouhani's first term (2013–2017), the security budget increased by 1,200 percent.[3] Frank Cillufo, director of the Center for Cyber and Homeland Security and the vice president of George Washington University, declared 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 operations into their military strategy and doctrine."[4]

Two major events were pivotal in the development of Iranian activities in cyberspace. The first is the internal civilian protest that took place in 2009, known as the "Green Movement" and coined the "Twitter Revolution" by

1 "The Israel National Cyber Directorate: Iran Is a Main Cyber Threat on the Middle East," *Israel National Cyber Directorate*, June 26, 2019, https://www.gov.il/en/departments/news/unna_cyber_week_2019.

2 Robert McMillan, "Iranian Hackers Have Hit Hundreds of Companies in Past Two Years," *Wall Street Journal*, March 6, 2019, https://www.wsj.com/articles/iranian-hackers-have-hit-hundreds-of-companies-in-past-two-years-11551906036.

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

4 Sam Cohen, "Iranian Cyber Capabilities: Assessing the Threat to Israeli Financial and Security Interests," *Cyber, Intelligence, and Security* 3, no. 1 (2019): 71–94.

foreign media outlets. In the wake of the Iranian presidential election of 2009 and the disclosure of Ahmadinejad's victory over his main opponent Mousavi, massive protests took place across Iran to challenge the election's results.[5] Claiming that the election was rigged, the protestors wore green, the color of Mousavi's campaign, which gave name to the protest movement. Despite the regime's repression, the protestors were active for many months after the election. They concentrated their efforts on utilizing social media channels, such as Twitter, Facebook, and YouTube, for organizational purposes and as a platform to convey updates and information both inside and outside of the country. This remarkable use of information and communication technologies (ICT) helped to strengthen the movement while the government struggled to thwart its activity. This situation forced the Iranian regime to improve its understanding of cyberspace and its proficiencies to operate in this field. The development of a cyber strategy became a vital necessity.

The second major event—the attack known as "Stuxnet"—is considered decisive in the pursuit of a national plan to build Iran's cyber capabilities. The Stuxnet malware was discovered in 2010 and targeted Iranian computer systems.[6] The exact activity of Stuxnet remains unclear, suggesting a longer operating period from its conception to its disclosure.[7] It caused the self-destruction of almost a thousand centrifuges—around a fifth of all active centrifuges at the Natanz's nuclear enrichment facility, significantly delaying the Iranian nuclear program.[8] The impact of this malware exposed the vulnerability that states have experienced with the increased interconnectedness of most of the critical sectors. The emergence of new technologies also emphasized the need for enhanced security needs to protect and defend states in cyberspace.

In addition, economic pressure and the impediment of the nuclear program fostered social and economic resilience. The Iranian utility to turn to resilience seems to be by using "hybrid tools," including cyber activities. To this end, the development of cyber capabilities should be seen in many

5 "Editorial: Iran's Twitter Revolution," *Washington Times*, June 16, 2009, https://www.Washingtontimes.Com/News/2009/Jun/16/Irans-Twitter-Revolution/.

6 Josh Fruhlinger, "What Is Stuxnet, Who Created It and How Does It Work?," *CSO*, August 22, 2017, https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html.

7 "The Israel National Cyber Directorate: Iran is a Main Cyber Threat on the Middle East."

8 Taylor Armerding, "Whatever Happened to Stuxnet," *Synopsy*, January 17, 2019, https://www.synopsys.com/blogs/software-security/whatever-happened-to-stuxnet/.

ways as a means of the Islamic regime for competing against its internal and external adversaries.

The following section will examine facts, events, figures, and official statements in order to identify common patterns and comprehend Iranian cyber activity. These characteristics will then enable analysis and understanding of Iran's presumed cyber strategy.

Confronting External Adversaries

Over the years, the Iranian regime has set up a cyber array that includes organized hacker groups operating under its various security organizations and independent groups operating in the interest of the regime. In addition, several groups and states in the Middle East receive Iranian support and function effectively as envoys operating on behalf of Iran's cyber interests. This aim of this section is to understand Iranian cyber actions and how they help to comprehend the regime's cyber strategy.

Operation Abadil is considered one of Iran's most destructive attacks and is part of a defensive strategy against the United States. The campaign launched in 2012 is still active and includes different versions and waves of DDoS attacks.[9] The first wave targeted the US financial system by attacking American banks, which were not prepared for such traffic at the time. The attack blocked the banks' websites and servers and prevented customers from using online banking services. Izz ad-Din al-Qassam Cyber Fighters, which are allegedly linked to the Iranian government, claimed responsibility for this attack. In this case, Iran utilized cyber force through a state-sponsored actor against one of its main enemies—the American financial establishment.

In 2012, the destructive malware, renamed "Shamoon," breached the Saudi Arabian oil giant Aramco and affected Saudi computer systems, causing great damage and recovery costs. Attacks against Saudi strategic targets and allies in the region, such as RasGas in Qatar, should be considered part of the Iranian defensive strategy in cyberspace.[10] In 2016, other versions of the malware attacked new targets, especially government ministries, such as the Ministry of Labor, and companies in Saudi Arabia, such as the

9 "Operation Abadil DDoS attack," *Radware*, https://security.radware.com/ddos-experts-insider/expert-talk/ddos-attacks-operation-ababil/.

10 "Operation Cleaver," *Cylance* (2014), 1–86.

Saudi Central Bank.[11] In 2018, new waves of the malware targeted critical industries (oil, energy, telecommunication) and government organizations throughout the region.

In May 2016, it was reported that an Iranian state-sponsored organization had used websites and servers to attack about 120 Israeli organizations and institutions;[12] later identified as the OilRig[13] hacker group, it has operated on behalf of the Iranian government since 2015. In May 2017, the same hacker group, using Russian-based attack tools, attacked computer systems belonging to an American contracting firm engaged in security.[14] The company's security experts noted that this was the first case of cooperation between Iranian and Russian hackers who sold their services at the highest cost. This attack also revealed a significant upgrade in the capabilities of Iranian hackers. A few months later, the US Treasury indicted the Ajily Software Procurement Group as an international crime organization. The Iranian-based group had used hackers to steal engineering software that could be used to design GPS-guided weapons from the United States and other Western countries.[15] This attack was part of Iran's defensive initiative against the economic restrictions imposed by the United States. Contrary to the previous cases discussed here, this case dealt with theft and business espionage and demonstrates how the Iranian government has used cyber force to circumvent US sanctions in order to import military technology.

In June 2014, it was revealed that an Iranian cyber terrorist group affiliated with the Iranian Revolutionary Guard Corps (IRGC) had been attacking hundreds of targets in Israel and the Middle East for about a year. The hacker group was called "Ajax Team" or "Rocket Kitten" and had been operating within the Iranian security organizations in recent years.[16] The multi-stage

11 Collin Anderson and Karim Sadjadpour, *Iran's Cyber Threat: Espionage, Sabotage and Revenge* (Washington DC: Carnegie Endowment for International Peace, 2018), 1–57.

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

13 Bryan Lee, Robert Falcone, "Behind the Scenes with Oil Rig," *Unit 42*, April 30, 2019, https://unit42.paloaltonetworks.com/behind-the-scenes-with-oilrig/.

14 Nicole Perlroth, "Web Defenders Detect Russian Hand in Iranians' Hacking Attempt," *New York Times*, May 15, 2017, https://www.nytimes.com/2017/05/15/technology/web-defenders-detect-russian-hand-in-iranians-hacking-attempt.html.

15 "Ajily Software Procurement Group," *Iran Watch*, August 8, 2017, https://www.iranwatch.org/iranian-entities/ajily-software-procurement-group.

16 Check Point, *Rocket Kitten: A Campaign with 9 Lives* (2015), 1–38.

attack targeted a variety of channels, including Israeli scientists, embassy staff, NATO officials, Iranian dissidents, the Saudi royal family, and others. The purpose of the attack was to gain access and steal critical information. Experts estimated that this was a highly targeted, sophisticated, tenacious, and systematic attack system, based on intelligence gathering and focused information on the targets. In November 2015, the IRGC broke into the emails and social networks of members of former US president Barack Obama's administration, while Facebook confirmed that it had identified attempts to take over profiles of government employees.

ClearSky's cyber intelligence company published a report in July 2017 about an Iranian cyber intelligence operation known as "Wilted Tulip."[17] In this operation, the Iranian hackers known as "CopyKittens" managed to gain access to information from a number of government agencies in Israel.[18] The hackers used a variety of methods, including the Watering Hole attack, which involves breaking into news sites, infecting them, and sending links to various victims under the guise of legitimate articles in order to gain control of their computers. In order to gain the trust of the victims and make them click on the links to the infected sites, the group used a relatively complex and authentic network of profiles on Facebook, some of which had been around for years. To support the authenticity of those profiles, several websites (built with an Iranian website building platform) and business pages on the social network had been set up. Its victims included government agencies and private companies in several Middle Eastern countries such as Israel, Saudi Arabia, and Turkey, as well as Western countries, such as the United States and Germany.

In 2018, using a malware nicknamed "Madi," Iran attacked Israeli targets, in addition to US think tanks, companies, and academics, in order to steal information and documents from over 800 victims.[19] In November 2019, Microsoft declared that it had identified intense cyber activity by a hackers' group called "Phosphorous," allegedly linked to the Iranian government.[20]

17 Eduard Kovacs, "Iranian CopyKittens Conduct Foreign Espionage," *Security Week*, July 25, 2017, https://www.securityweek.com/iranian-copykittens-conduct-foreign-espionage.

18 Clearsky Security and Trend Micro, *Operation Wilted Tulip* (July 2017), 1–48.

19 GReAT, "The Madi Campaign – Part I," Kapersky, July 17, 2012. https://securelist.com/the-madi-campaign-part-i-5/33693/.

20 "Microsoft: Iranian Hackers Targeted a US Presidential Campaign," *Asharq Al-Awsat*, October 4, 2019, https://aawsat.com/english/home/article/1931446/microsoft-iranian-hackers-targeted-us-presidential-campaign.

This cyber operation targeted current and former US government officials, journalists, Iranians living outside Iran, and potential candidates for the 2020 US presidential election, although they were not specified. It consisted of more than 2,700 attempts to identify email accounts belonging to the specific targets, followed by attacks on 241 accounts.[21] This type of operation, which aimed to interfere in foreign election campaigns, has become a significant concern since the American administration concluded that Russia had succeeded in disrupting the 2016 election process. This attempt to disrupt foreign elections and to target people outside of Iran appears to be part of Iran's offensive operation.

Confronting Internal Adversaries

Despite recent calls to restrict access to the internet, Iran already implemented measures allowing the regime to control people's access to connectivity. Indeed, the government uses its control over the internet's access as a means of disrupting communication in the country, especially during times of popular unrest. Since 2009, each mass protest has led the regime to impose restrictions on internet access.[22] In November 2019, after the government announced a considerable increase in gasoline prices, civil protests exploded in Tehran and other cities; the Iranian security forces responded violently and repressively, and a nationwide shutdown of the internet was imposed for almost a week, which completely disconnected the Iranians. This protest was a relevant example of Iran's use of its power in cyberspace for internal purposes: preventing its population from communicating, organizing, sharing information, and protesting.[23] The authorities' efforts to block the internet and restrict people's access to communication platforms in general and to develop a national internet project have been amplified by attempts to limit the use of VPNs (virtual private network) among the population. For instance, the Iranian government has obliged web services to sign a pledge stating that the "establishment and distribution of VPN and proxy services"

21 "Microsoft: Iranian Hackers Targeted a US Presidential Campaign."

22 Borzou Daragahi, "Massive Iranian Internet Shutdown Could Be Harbinger of Something Even Darker to Come, Experts Warn," *The Independent*, November 30, 2019, https://www.independent.co.uk/news/world/middle-east/iran-internet-shutdown-protests-communications-tehran-a9226731.html.

23 Amy Slipowitz, "The True Depth of Iran's Online Repression," *Freedom House*, December 2, 2019, https://freedomhouse.org/blog/true-depth-iran-s-online-repression.

are forbidden.[24] In addition to trying to prevent people from using VPNs, Iran is apparently trying to create a national VPN regulating the access to the internet for each individual based on profession, according to a statement of Hamid Fattahi, the CEO of the government-owned Telecommunications Infrastructure Company (TIC), on November 11, 2019.[25]

Since 2005, the Iranian regime under President Khatami has been advocating the idea of a closed and national network.[26] Beginning in 2010, the project of creating a "halal internet" network for Iran was introduced, with the aim of upholding Iranian values and preventing foreign threats from entering the regime's network, while it would also enable the authorities to control internal actors and monitor potential dissidents.[27] This initiative appeared shortly after the disclosure of the Stuxnet attack and was seen as an effort to respond to the new risks and threats that Iran faced at the time. Despite skepticism of observers regarding the success of such a project, other countries decided to adopt the same tactic; Russia, for example, passed a law in November 2019 that enabled the state to create an internet for Russian users only, which is completely closed to external actors and controlled by Russian authorities, indicating the real motive of such a project.[28]

This "halal internet," also known as the Iran National Information Network (SHOMA), is developing within the context of increasing surveillance of the population on the internet.[29] Indeed, calls of Iranian officials for greater surveillance and restrictions of the internet are repeatedly heard, and President Rouhani is often targeted by conservatives who accuse him of being weak

24 "State-Developed VPN Would Determine Iranians' Internet Access Based on Their Job," *Center for Human Rights in Iran*, November 21, 2019, https://iranhumanrights.org/2019/11/state-developed-vpn-would-determine-iranians-internet-access-based-on-their-job/.

25 "State-Developed VPN Would Determine Iranians' Internet Access Based on Their Job."

26 Julie Kebbi, "Internet: l'Autre repression du régime iranien," *L'Orient-le-jour*, November 22, 2019, https://www.lorientlejour.com/article/1195979/internet-lautre-repression-du-regime-iranien.html.

27 Christopher Rhoads and Farnaz Fassihi, "Iran Vows to Unplug Internet," *Wall Street Journal*, May 28, 2011, https://www.wsj.com/articles/SB10001424052748704889404576277391449002016.

28 Lucie Bras, "Russie: à quoi va ressembler le « Runet », le nouvel internet 100% russe contrôlé par Moscou?," *20Minutes*, November 5, 2019, https://www.20minutes.fr/high-tech/2644575-20191105-russie-quoi-va-ressembler-runet-nouvel-internet-100-russe-controle-moscou.

29 Amy Slipowitz, "The True Depth of Iran's Online Repression," *Freedom House*, December 2, 2019, https://freedomhouse.org/blog/true-depth-iran-s-online-repression.

and not responsive enough to the evolving threat that the internet poses.[30] For example, Attorney General Mohammad Jafar Montazeri called in May 2019 for stronger surveillance and more restrictions of the internet. He directly warned Minister of Information and Communications Technology Mohammad Javad Azari Jahromi,[31] apparently seen as too reformist, that he should be held accountable for delays in implementing new reforms and for not launching the "national internet" as desired by the Supreme Leader Ali Khamenei.

In parallel to the multiple restrictions that Iran has placed on foreign communication giants such as Telegram (messaging service application), the regime has helped to develop alternative platforms by providing technical support and financial resources to Iranian messaging applications Soroush and Bale, which operate at the national level. An indication that Iran was willing to foster the creation of local apps was in 2017 when it launched grant incentives of more than $200,000 USD for software developers able to reach a million users on their communication platform.[32] Government bodies benefit from weak data privacy policies that enable them to collect and store users' data, representing a potential danger for customers.[33] As the Iranian regime uses its power to regulate the use of the internet among the population, it both censors the internet and creates alternatives to exercise a strengthened control over it.

Analysis of the Iranian Cyber Operations and Force Build Up

Since the end of the 2000s, the developments of cyber risks and threats against the Islamic regime have fueled Iranian interests in cyberspace. Iran has invested a significant amount of resources to operate in cyberspace—

30 "En Iran, la justice appelle à davantage de surveillance sur Internet," *Le Monde*, May 4, 2019, https://www.lemonde.fr/keyhani/article/2019/05/04/en-iran-la-justice-appelle-a-davantage-de-surveillance-sur-internet_5994643_5470831.html.

31 "Iran Prosecutor Warns Minister to Tame Social Media or Face Consequences," *RadioFarda*, May 5, 2019, https://en.radiofarda.com/a/iran-prosecutor-warns-minister-to-tame-social-media-or-face-consequences-/29922128.html.

32 "In Iran, State-Sanctioned Messaging Apps Are the New Hallmark of Internet Nationalization," *Global Voices*, October 24, 2018, https://advox.globalvoices.org/2018/10/24/in-iran-state-sanctioned-messaging-apps-are-the-new-hallmark-of-internet-nationalization/.

33 "Pressure on Web Service Providers in Iran to Ban Proxies," *BBC Persia*, November 23, 2019, https://www.bbc.com/persian/iran-50531178.

which it refers to as an active battleground against the United States and its allies—and advances on multiple paths simultaneously: both to protect the regime against Western cultural attack and to physically destroy Western infrastructures.[34] The regime leads retaliatory operations against enemies that supposedly try to attack Iran, activities of cyber espionage to gain information on its adversaries' activity and capabilities, and offensives to disrupt them. At the eighth national civil defense forum held in Tehran in November 2019, the head of Iran's Civil Defense Organization, Brigadier General Gholamreza Jalali, announced that Iran was adopting a new defensive approach to the new hybrid and multi-layered threats and was developing defensive products to be used in cyberspace.[35]

The development of the cyber field signifies technological innovation and the strengthening of Iran's position in the international system as a regional technological power. The numerous resources that the Tehran regime invests in cyber have also born fruit in the civilian sector, while expanding the country's communications infrastructure to rural areas and increasing the speed of surfing in urban areas. The targets of Iran's cyberattacks are the regime's rivals inside the country, as well as its adversaries in the West and in the Middle East, including Israel and Saudi Arabia. Many of the targets are civilian-related organizations, such as security systems, private companies, academic actors, government officials, and public infrastructures. As in previous years, the Iranian cyberattacks continue to be effective due to the high level of planning of the operations and the systematicity in which they are carried out. Although the Iranian attacks are not technologically sophisticated, the technical level of the attacks has increased significantly in recent years.[36]

The following section will identify four main patterns that characterize the Iranian strategy in cyberspace. The first consists of a tit-for-tat strategy in terms of cyber defensive and offensive activities based on geopolitical developments as a pattern of the offensive operations against external adversaries. The second consists of developing internal cyber capabilities

34 Author's opinion based on research.

35 "Iran Opts for New Civil Defense Approach to Confront US Threats," *Fars News Agency*, November 5, 2019, https://en.farsnews.com/newstext.aspx?nn=13980814000432.

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

in order to build an economic resilience; that is, being part of the world economy despite international sanctions and participating in technological innovation. This will be categorized as a pattern of the Iranian internal strategy in cyberspace with both offensive and defensive initiatives. The third aspect of the cyber strategy corresponds to the regime's set of values, religion, and cultural rules, as part of an offensive and defensive strategy applied both internally and externally. Finally, the fourth characteristic could be explained as the full exploitation of both the cyber toolkit and the lack of a legal framework distinguishing cyber from other fields of activity, enabling Iran to strengthen its offensive strategy against internal and external adversaries.

Tit-For-Tat Strategy of Adapting to the Geopolitical Context

Soon after the disclosure of the Stuxnet virus, Iran accelerated its pursuit of its operation in cyberspace. Two years later, the US economic sanctions led the Islamic Republic to attack its American rival in the cyber field. Iranian strategy in cyberspace should be considered a tit-for-tat strategy as it adapts its responses to geopolitical tensions at a regional or international level as part of its external offensive strategy in cyberspace. The use of offensive activities in cyberspace to respond to geopolitical events has been a steady mechanism in Iran. This trend means that Iranian cyber strategy is linked, if not dependent on, its geopolitical interests and adapts the strategy to them. This is an interesting element in comprehending Iranian cyber strategy as other countries do not especially design their cyber strategy in response to geopolitical developments (for example, China or Russia).[37]

The United States considered Operation Abadil as the most significant attack allegedly launched by Iran in order to counter US-imposed international economic sanctions following the development of Iran's nuclear program. This attack was considerable, given the level and intensity of the attacks. In 2016, the US Department of State indicted seven Iranian individuals, who were linked to the Iranian Revolutionary Guard Corps for participating in the attack.

The characteristic of Iran's adapting its cyber strategy to geopolitical developments has been observed in the negotiations for the Joint Comprehensive Plan of Action (JCPOA). US officials commented that Iran conducted cyber

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

operations that caused significant damage to companies in the West and to Iran's enemies in the Middle East in 2013 and 2014, the period leading up to the agreement.[38] A clear increase in the number of Iranian offensive attacks in cyberspace can be discerned when sanctions were applied, while the JCPOA had a real impact on Iran's cyber strategy as the frequency and scale of attacks decreased with the nuclear deal's signature. When President Trump announced his decision to withdraw from the JCPOA in May 2018, it had the opposite effect. Less than twenty-four hours later, Iran had launched an aggressive campaign of phishing emails sent to US allies abroad. The level of preparation needed for this attack indicated that the Iranian forces had actually prepared the attack before Trump's announcement and chose to undertake the operation as a response to his decision. Indeed, experts identified a resurgence of cyber offensive activities coming from Iran, signifying a real shift in policy.[39] According to cybersecurity experts, Iranian efforts to target American facilities and individuals in cyberspace intensified after 2018 and following the US withdrawal from the JCPOA.[40]

Iran's activities outside the country through the support of proxies should also be included in this tit-for-tat strategy. The second wave of the Shamoon operation in 2016–2017 included references to Yemen and an image of the Syrian child Alan Kurdi appeared on targeted devices and was observed as retaliation for Saudi activities in Syria and Yemen. Recently, in June 2019, CrowdStrike and FireEye also stated that Iranian offensive cyber operations had intensified.[41] This offensive came shortly after the Trump administration imposed new sanctions on the Iranian petrochemical sector. According to CrowdStrike, "Refined Kitten," —the hackers' group that is thought to have instigated this cyber offensive—has been targeting the American defense and energy industries for years. In September 2019, Iran was accused of undertaking the attack against Aramco; however, Iran denied it and accused

38 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/.

39 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.

40 "Iranian Hackers Wage Cyber Campaign amid Tensions with US," *Asharq Al-Awsat,* June 22, 2019, https://aawsat.com/english/home/article/1779921/iranian-hackers-wage-cyber-campaign-amid-tensions-us.

41 "Iranian Hackers Wage Cyber Campaign amid Tensions with US."

the Houthis (Zaydi Shiites in Yemen).[42] This attack had a significant impact on the largest oil producer and delayed oil production. It happened just after US officials declared they attacked Iran in a covert campaign in June 2019.

Building a Resilience: Circumventing Economic Pressure and Leading a Cyber Revolution

Despite the creation of new cyber bodies and implementation of cyber regulation, the Iranian government seemingly invests in the education of future generations[43] as part of an offensive strategy aiming to build internal cyber capacities. Iran has massively invested in the cyber field by creating new official organizations and infrastructure and a considerable part is also dedicated to education. The government, as well as non-state actors, apparently recognize the importance of educating people in cyber; for example, several Iranian universities offer hacking classes.[44] Educating a large number about cyber technology is likely to support the industry's development and perhaps to enhance people's commitment to the state in this field.[45] Since attribution is difficult in cyberspace, unofficial state-related groups can operate on behalf of the interests of the state. Iranian decision makers realized the significance of this phenomenon, of investing large amounts of money to educate people, with the expectation that they would eventually commit to supporting the state. Although the investment in education will not systematically be translated into new public employees, it could lead to the formation of self-motivated groups. In addition, the government has shown interest in supporting start-ups and innovation. In September 2019, the Iranian government decided to invest $225 million USD in the Iran Innovation Fund for supporting innovation and encouraging start-ups.[46]

Developing its cyber capabilities to become a leader in cyberspace also implies that Iran engages in cyber espionage in order to steal rivals' technology and to gain information about their capabilities. The Madi malware in 2012,

42 Bruce Riedel, «Who are the Houthis, and why are we at war with them?» *Brookings*, December 18, 2017, https://www.brookings.edu/blog/markaz/2017/12/18/who-are-the-houthis-and-why-are-we-at-war-with-them/.

43 Veronika Netolická and Miroslav Mareš, "Arms Race 'in Cyberspace' – A Case Study of Iran and Israel," *Comparative Strategy* 37, no. 5 (2017): 414–429.

44 "Threat Intelligence Briefing Episode 11," *HP Security Research,* February 2014.

45 Netolická and Mareš, "Arms Race 'in Cyberspace."

46 "Iran Gov't Invests $225m in Innovation Fund," *Financial Tribune*, September 6, 2019, https://financialtribune.com/articles/sci-tech/99750/iran-gov-t-invests-225m-in-innovation-fund.

the Rocket Kitten activities in 2014, and the attempts of the Ajily Software Procurement Group to illegally import American stolen software to Iran are all relevant examples of Iranian cyber espionage activities. Iranian activities to gain technological power are usually accompanied by disruptive activities designed to target foreign critical infrastructures, especially in the energy and defense fields, as was illustrated by the APT33 threat actor (also known as Elfin) for many years.[47]

The development of cyber capabilities might also serve as a means of circumventing economic pressure and diversifying sectors of the economy as part of a defensive strategy. Indeed, building and improving cyber capabilities also means developing new technological tools. The cryptocurrencies, which are completely digitalized, could embody the economic tools of cyberspace. For now, crypto trading is still forbidden in the Islamic Republic, but cryptocurrency mining was recently authorized and legislated as an industrial activity.[48] Iran's Ministry of Industry, Mine, and Trade has the full authority to give approvals to local miners, and some rules were designed to regulate this activity. The new law was passed in Iran at a time when Iranians already operated crypto mining as a way of avoiding economic sanctions. Even if the law limits the geographical areas in which it is allowed to mine and obliges individuals to pay charges for the electricity consumed, Homayun Haeri, the deputy minister of energy, has declared that the government will vote on a measure to apply lower electricity rates for mining farms. This kind of measure is likely to foster mining activities in Iran. This pronouncement sounds suspicious, however, since the Central Bank has recommended banning the payment of cryptocurrencies within Iran, whereas civil society and companies have tried to promote cryptocurrencies at a domestic level. If Iran is developing this tool to counter international economic sanctions, the United States has already taken action against two Iranians who allegedly facilitated payments for the SamSam malware. The State Department Office of Foreign Asset Control put the two on its sanctions list for bitcoin activities, meaning they are blacklisted and cannot send money to individuals and

47 "Elfin: Relentless Espionage Group Targets Multiple Organizations in Saudi Arabia and U.S.," *Symantec*, March 27, 2019, https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage.

48 Marie Huillet, "Iranian Govt Authorizes Cryptocurrency Mining as Industrial Activity," *Coin Telegraph*, July 29, 2019, https://cointelegraph.com/news/iranian-govt-authorizes-cryptocurrency-mining-as-industrial-activity.

services or receive from them.[49] Furthermore, in December 2019, President Hassan Rouhani proposed the creation of a Muslim cryptocurrency as a mean of fighting against American economic hegemony. This was the first time the Iranian regime publicly announced it was creating cryptocurrency in order to avoid the use of the US dollar as part of a defensive financial strategy.[50]

Protecting the Regime's Stability and Spreading its Values

After the 2009 Green Movement, Iran realized the danger of new technologies in terms of organizing resistance and a potential rebellion. As the country reacted to this phenomenon, it developed a defensive and offensive strategy in cyberspace, applied both internally and externally. The regime tried to regulate activity in cyberspace and to control the content shared as part of defensive operations inside the country. According to a survey published in 2012, 27 percent of websites were then blocked in Iran,[51] as they were considered to be against Muslim values. Indeed, there is a national ban of most of the social networks, including Facebook and Twitter.[52] According to an interview with Prosecutor Ahmad Ali Montazeri, who presides over the Internet Censorship Committee, Iran banned 14,000 websites and social media accounts weekly in 2016.[53] He explained that the content of these websites, which opposed Iranian values and religion, justified their closure, adding that the country was under attack by foreign and hostile media. This victimization tactic has been used at times in Iran to apply censorship and spread propaganda. In 2017, 2018, and 2019, during the Iranian popular protests, the regime blocked some websites and communication platforms.

---

49 "US Regulators Tie Two Bitcoin Addresses to Iranian Ransomware Plot," *CoinDesk*, November 28, 2018, https://www.coindesk.com/us-regulators-tie-two-bitcoin-addresses-to-iranian-ransomware-plot.

50 Helen Partz, "Iran Wants to Create Crypto to Confront 'Economic Hegemony' of US," *CoinTelegraph*, December 19, 2019, https://cointelegraph.com/news/iran-wants-to-create-crypto-to-confront-economic-hegemony-of-us.

51 "Current State of Internet Censorship in Iran," *View DNS.info*, March 23, 2012, https://viewdns.info/research/current-state-of-internet-censorship-in-iran/.

52 Leyla Khodabakhshi, "Why Ordinary Iranians Are Turning to Internet Backdoors to Beat Censorship," *BBC News*, January 10, 2018, https://www.bbc.com/news/blogs-trending-42612546.

53 "Iran Bans 14 Thousand Websites and Accounts Weekly," *Al Arabiya*, December 8, 2016, https://english.alarabiya.net/en/media/digital/2016/12/08/Iran-bans-14-thousand-websites-and-accounts-weekly-.html.

The authorities even cut off internet access in some places.[54] For example, the government blocked Telegram, one of the most used communication apps among Iranians. Indeed, Iranian officials, who apparently learned from previous events, were willing to prevent civil society from communicating, informing, and organizing itself through this platform.

Maintaining Iran's culture is important for Iran in its drive to develop cyber capabilities and is a pattern of its strategy. The cultural factor is reflected in Iran's cyber activities, as many attacks led by Iranian actors have been linked in one way or another to religious or cultural justifications. Pride is also likely to be a reason why Iran wants to lead the region and the world in terms of technological innovation.[55] Jalali, the head of Iran's Civil Defense Organization, highlighted in November 2019 the prominent role that Iran has in the field of cyber, adding that the regime developed cyber defense before any other countries, including the United States, and that many countries, such as Russia and North Korea, were willing to receive training from Iranian cyber forces.[56] The sense of national pride related to the role of being a leader in the technology field is crucial to understanding Iran's strategy in cyberspace. Since around 2010, Iran has succeeded in expanding internet access to rural areas and to improving connectivity in cities,[57] making it one of the Middle Eastern countries with the largest number of internet users.

The regime is also committed to spreading its values outside the country, as part of an offensive operation against its "enemies." FireEye, a cybersecurity company, identified a campaign promoting Iranian political narratives in 2018.[58] The operation included the use of illegitimate news websites and the abuse of social media. The cybersecurity company analyzed it as a replication of Russian attempts to influence foreign public opinion during the 2016 US presidential election. In September 2019, Gholamreza Soleimani,

54 "In Response to Protests, Iran Cuts Off Internet Access, Blocks Apps," *NPR*, January 3, 2018, https://www.npr.org/2018/01/03/575252552/in-response-to-protests-iran-cuts-off-internet-access-blocks-apps.

55 Gawdat Bahgat and Anoushiravan Ehteshami, "Iran's Defense Strategy: The Navy, Ballistic Missiles and Cyberspace," *Middle East Policy Council* 24, no. 3 (2017): 89–103.

56 "Iran Opts for New Civil Defense Approach to Confront US Threats," *Fars News Agency*, November 5, 2019, https://en.farsnews.com/newstext.aspx?nn=13980814000432.

57 Anoushiravan Ehteshami, "Iran: Stuck in Transition," *Journal of International and Global Studies* 9, no. 2 (2017): 186–188.

58 Ed Parsons and George Michael, "Understanding the Cyber Threat from Iran," *MWR Info Security*, 17 April 2019, https://www.f-secure.com/en/consulting/our-thinking/understanding-the-cyber-threat-from-iran.

commander of the Basij organization, announced the creation of one thousand cyber battalions around the country, via pro-regime user accounts on social media.[59] A battalion is composed of around five-hundred soldiers, meaning that the regime probably launched more than half a million pro-regime accounts. He stayed silent regarding the means and budget used by the Basij organization to achieve this project. Soleimani also stated that "the enemy has expressed concern over the organized presence of revolutionary youth in cyberspace on several occasions, and that reflects the momentum that has been created. This presence will expand and be enhanced." However, despite this new initiative aiming to spread pro-regime views on the internet, Iran is likely to face difficulties since Twitter has been removing thousands of state-backed accounts lately (including accounts believed to be linked to the Iranian government).

Besides Iran's determination to protect its system of values, the regime also has attempted to fight against foreign ideas and has spread its propaganda through cyberattacks. For example, during Operation Abadil, hackers demanded the removal of "Innocence of Muslims," a movie distributed in 2012 and considered as offensive to Muslims' honor.[60] The cyberattack was accompanied by a cultural vindication because Iran's image had been insulted. Another example of spreading propaganda through a cyberattack was the Shamoon malware attack in 2016. During this operation, infected devices were smeared with anti-Western images, such as an American flag burning. Another version of Shamoon later reappeared and spread the malware with a verse of the Quran in infected devices.[61]

Taking Advantage of Cyberspace's Characteristics

Cyberspace is a privileged area in which Iran and non-liberal countries do not play by the same rules as do democratic countries, such as the United States and Israel. Indeed, they do not submit to the same rules and Iran appears to take advantage of this difference in its offensive strategy against both

59 "Nouveaux cyber-brigades en Iran," *PressTV*, September 7, 2019, https://www.presstv.com/DetailFr/2019/09/07/605586/Des-cyberbrigades-en-Iran.

60 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.

61 Charlie Osborne, "Shamoon Data-Wiping Malware Believed to Be the Work of Iranian Hackers," *ZDnet*, December 20, 2018, https://www.zdnet.com/article/shamoons-data-wiping-malware-believed-to-be-the-work-of-iranian-hackers/.

internal and external adversaries. Since they do not adopt the same values, Iran considers some practices acceptable and others as ethically and morally forbidden. In contrast, the Western, democratic, and developed countries act according to the legal framework of their countries. They also tend to adopt and respect international law, because they greatly value the public opinion.

As a non-liberal regime, Iran allows itself to regulate and censor cyberspace in an extremely restrictive way, depriving its citizens of basic tools for connecting with the world. Information regarding national activities in cyberspace is also kept hidden from the public. While democracies generally avoid ambiguity, out of their duty to respect legal principles, it is fully used by authoritarian regimes such as Iran. Iran remains very opaque when it comes to cybersecurity and information activities, whereas democracies must remain highly transparent and will be held accountable for any kind of decision made. Rejecting the concept of accountability, Iranian officials benefit from wider freedom of action, without generally fearing the population's disapproval. This is especially the case when Iran attempted to infiltrate American and European networks through the operation led by the Phosphorous group, which was discovered by Microsoft in September 2019. Similar to Russian activities in 2016, Iran apparently has tried to influence foreign elections, attacking potential candidates of the 2020 presidential election.

The ambiguity and deniability of cyberattacks allow attackers to use cyber warfare via covert operations. It makes cyberspace a privileged area to confront enemies without fearing direct retaliation. The activity of hackers' groups whose links with the Iranian government are ambiguous is another issue. Cooperation with foreign groups is also an evolving phenomenon of Iran's cyber activities, which enables Iran's denial. Indeed, the OilRig's use of Russian cyber tools to attack an American target in 2017 illustrated the coordination between Russian and Iranian hackers. Another aspect of the deniability of cyberattacks is the importance of proxies through state or non-state actors that are supported by Iran and that conduct activities on their own in agreement with Iranian interests. Proxies of Iran are spread all over the region, both within Shiite and Sunni forces (Houthis in Yemen, Hamas in Gaza, Hezbollah in Lebanon, and so forth). Due to the ambiguity caused by the proxies' activity, Iran easily denies involvement in cyber operations, as it rejected the accusation of attacks against Saudi facilities in September 2019, claiming the Houthis' responsibility for this operation.

The last pattern identified as part of Iran's national cyber strategy is its deniability of being targeted by attacks. Indeed, public statements by Iranian government officials claiming that Iran is impervious to cyberattacks are common. A recent example of these declarations is in an interview with Jalali, published in November 2019, who said that foreign attempts to attack Iran in cyberspace had been unsuccessful for the past two years a result of the effectiveness of defensive cybersecurity mechanisms.[62] At the same time, US officials claimed the success of a covert cyber operation in Iran, which affected the regime's ability to target oil tankers in the Persian Gulf in June 2019.[63] In fact, Minister of Communications and Information Technology Mohammad Javad Azari Jahromi even declared that the United States "must have dreamt" about the operation.[64]

Conclusion

Iran currently poses a major cyber threat to the international system. The actions of the Islamic Republic and the strategy behind it have led Western government officials and experts from the private sector to believe that Iran seeks to stand alongside cyber powers, such as Russia and China. Should Iranian capabilities continue to evolve, experts say that an attack that could damage physical infrastructure is likely.

The offensive cyber strategy of Iran can be described as a tit-for-tat strategy, based upon cultural justification, pride, and benefits from cyberspace particularities. Iran has emerged among major global cyber actors. The reputation that the Islamic Republic has acquired serves its strategy and its efforts to use asymmetrical warfare against its external adversaries. The Iranian regime invests a great number of resources in developing the country's cyber capabilities in a variety of fields and subsequently strengthens its field of defense. This field also benefits from civilian investments where Iranian institutions such as Sharif University are highly regarded.

Iran's defensive strategy is led by its need to build economic and technological resilience as well as by its determination to neutralize internal and external threats. The regime recognizes the importance of establishing

62 "Iran Opts for New Civil Defense Approach to Confront US Threats," *Fars News Agency*, November 5, 2019, https://en.farsnews.com/newstext.aspx?nn=13980814000432.

63 Julian E. Barnes, "U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say," *New York Times*, August 28, 2019, https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html.

64 Barnes, "U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say,"

defensive capabilities alongside attack capabilities. In addition, it invests great efforts in acquiring surveillance capabilities and monitoring internet activity in order to maintain government integrity, aided by expert attackers from its natural partnerships with China, Russia, and North Korea.

Analysis of recent cyberattacks attributed to Iran shows that the regime has targeted a wide range of enemies, including Iranian dissidents inside and outside Iran, its close neighbors, such as Israel and Saudi Arabia, and distant countries such as the United States and the European states. Even if it cannot be compared to the United States or Israel, Iran is improving its cyber capabilities. Iran's cyberattacks have become more focused over the past two years; they involve the use of a wide range of tools and methods and are clearly designed and executed with a high degree of professionalism and patience worthy of bridging the technological gaps and increasing their effectiveness. Whether Iran has benefited or lost in terms of its offensives efforts against its external adversaries requires a barometer of consensus, while indicators may include national and defensive infrastructure and the public rhetoric.

Ambiguous Approach—All Shades of Gray

Raša Lazović

This essay aims to examine conflicts in the "gray zone." The paper is divided into three sections. The first section describes the gray zone and defines the ambiguous approach that corresponds to it. It argues that measures short of war, coercive gradualism, and deliberate obscurity are the crucial ingredients of the ambiguous approach. The second part discusses the ambiguous approach as a dependent variable, identifying the lack of power and lack of legitimacy to use force as the key drivers for adopting the ambiguous approach. Finally, the third section explores how actors can disrupt their opponent's strategic calculation by creating ambiguity around key components of the game: the players, their actions, outcomes of interactions, and information relevant to decision making.

Keywords: Gray zone, ambiguous approach, competition short of armed conflict, coercive gradualism, strategic ambiguity

Comprehending the Gray Zone and the Ambiguous Approach

Contemporary strategic-level challenges have blurred the clear distinctions between generally accepted concepts of war and peace.[1] Military force proves insufficient to address current asymmetric security challenges, and

Raša Lazović has worked at the Ministry of Defense of the Republic of Serbia. The opinions expressed in the article are the author's own and do not reflect the views or opinions of the Serbian government.

1 Nathan Freier and others, *Outplayed: Regaining Strategic Initiative in the Gray Zone* (Carlisle: SSI and US Army War College Press, 2016).

at the same time, the decision-makers' understanding of the thresholds that must be exceeded before actors engage in a full-scale military conflict is increasingly misleading and impractical.[2] It allows for near-peer fierce competition to extend into a vague space between war and peace, known as the "gray zone." Ongoing changes in the global strategic environment create favorable conditions for conflicts in this area.

Both challengers and status quo power perceive the gray zone as a useful playground for testing commitments and geopolitical competition while avoiding the risks and costs of an all-out war.[3] Indeed, several studies suggested that this type of conflict potentially could become the dominant form of state-on-state rivalry in the coming years.[4] In the context of this essay, "status quo power" refers to the United States. At the same time, the terms "revisionist" and "challenger" are used interchangeably and refer to emerging and resurgent global powers as well as to aspiring regional hegemons that are unsatisfied with the existing world order and eager to challenge the status quo power on a regional or global level.

The US military preeminence encourages revisionists to choose the gray zone as an alternative to the traditional military domain for geopolitical competition.[5] Playing by the rules, set by the status quo power, is not the way that challengers can change the existing balance of power. For the weak side, the primary rationale of moving the conflict into the gray zone is to change the rules of the game that underpin the current global order and to gain degrees of freedom of action. Revisionists seek to erode the status quo power deterrence, to paralyze its decision-making process, and to delegitimize the opponent's actions in order to equalize disparity in power.

The status quo power has to simultaneously address both threats that credibly challenge the rules currently defining the world order and the

---

2 Ben Connable, Jason H. Campbell, and Dan Madden, "Stretching and Exploiting Thresholds for High-Order War: How Russia, China, and Iran Are Eroding American Influence Using Time-Tested Measures Short of War," (Santa Monica: RAND Corporation, 2016), https://www.rand.org/pubs/research_reports/RR1003.html.

3 USSOCOM, "The Gray Zone," Public Intelligence, May 15, 2016, https://info.publicintelligence.net/USSOCOM-GrayZones.pdf.

4 Michael J. Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict* (Carlisle: SSI and US Army War College Press, 2015); Hal Brands, "Paradoxes of the Gray Zone," SSRN, 2016, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2737593.

5 Freier and others, *Outplayed*.

disruptive threats that arise from a disordered world.[6] By dragging conflict into the gray zone, the status quo power desires to preserve or to rebuild its freedom of action, and at the same time, it seeks to reduce the freedom of action of revisionists. It allows the status quo power to engage in competition short of armed conflict using all instruments of national power to keep initiative, avoid strategic overextension, and strengthen its deterrence.

There is no generally accepted name for gray zone campaigns. This essay uses the terms "ambiguous approach" and "ambiguous conflict" interchangeably and defines the ambiguous approach as a competition below that of armed conflict, which integrates measures short of war across multiple domains—obscure by design—aimed at gradually destabilizing, weakening, or delegitimizing an opponent in order to further national interests or shape the environment for future conflict. These three main concepts that characterize the ambiguous approach are further discussed below.

First, the ambiguous approach integrates measures short of war into a cohesive campaign. Measures short of war include any nonviolent or violent conflict action that actors use against each other to achieve and sustain strategic outcomes without engaging in high-end war. George Kennan divided these types of actions into two broad categories: measures of adjustment and measures of pressure.[7] While measures of adjustment are all part of the broader diplomatic repertoire, measures of pressure go beyond the regular practice accepted in relations between states. These measures can take many forms, including intimidation, subversion, psychological measures, economic pressure, election manipulation, support for political opposition, offensive cyber activities, using proxies, targeted killing, and many others. It is important to emphasize that the ambiguous approach requires the integration of these measures into a cohesive campaign in order to achieve a cumulative strategic effect.[8] Otherwise, it is unlikely these measures can accomplish anything more than purely tactical objectives.

Second, the ambiguous approach aims to gradually destabilize, weaken, and delegitimize the opponent and to create favorable conditions for future conflicts in an effort to pursue objectives that protect and promote the national

6 Kevin D. Scott, "Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World," *Joint Chiefs of Staff*, July 14, 2016, https://www.jcs.mil/Doctrine/Joint-Concepts/JOE/.

7 George Kennan, Giles Harlow, and George Maerz, *Measures Short of War* (Washington DC: National Defense University Press, 1991), 3.

8 Kennan, Harlow, and Maerz, *Measures Short of War*, 16.

interest. This coercive gradualism is a form of aggression in which the actor uses the step-by-step pursuit of his interests rather than a single *coup de main* against other nation's interests. By exercising coercive gradualism, with an indefinite time frame, actors employ different instruments of national power, exploiting the cumulative effect of incremental steps with the aim of creating a new strategic picture.[9] Contemporary examples of coercive gradualism are "salami-slicing" and limited *fait accompli*.[10]

Schelling points out that the key theme of a "salami-slicing" approach is that most of the commitments are ambiguous. That allows actors to challenge the seriousness of an opponent's commitment by using tactics of erosion. The challenge is usually low level or vague in order to avoid breaching the opponent's thresholds. If the opponent fails to react to a move, then the actor makes the next step, eventually accomplishing significant change in the status quo through steady incremental pressure.[11] The Chinese concept of "three warfares" and its application in the South China Sea is a typical example of a "salami-slicing" approach. By applying steady cumulative pressures across different domains, in the long run, they are seeking to produce a strategic outcome and avoid provoking a violent response.

On the other hand, when an actor applies a *fait accompli* approach, he makes a limited unilateral gain before anyone can react—thus confronting his opponent with the choice between conceding and escalating in retaliation.[12] As noted by Altman, the keywords are limited and unilateral. First, the gain has to be small enough not to provoke an overt military conflict. Second, by definition, *fait accompli* is a unilateral action that creates a new reality on the ground.[13] At this point, deterrence has already failed, and the opponent has no way back to the status quo *ante* without escalation of the conflict.

Both "salami-slicing" and limited *fait accompli* could cause uncontrolled escalation and, ultimately, all-out war. However, the decision to escalate is more complicated for the targeted state if the aggressor has local escalation

9 William G. Pierce, Douglas G. Douds, and Michael A. Marra, "Understanding Coercive Gradualism," *Parameters* 45, no. 3 (2015): 51.

10 Mazarr, *Mastering the Gray Zone.*

11 Thomas C. Schelling, *Arms and Influence* (Westport: Greenwood Press, 1977), 66–69.

12 Daniel W. Altman, "Red Lines and Faits Accomplis in Interstate Coercion and Crisis," (PhD diss., Massachusetts Institute of Technology 2015), https://dspace.mit.edu/bitstream/handle/1721.1/99775/927329080-MIT.pdf?sequence=1.

13 James J. Wirtz, "Life in the Gray Zone: Observations for Contemporary Strategists," *Defense & Security Analysis* 33, no. 2 (2017): 108.

dominance.[14] Russia's annexation of Crimea is the classic example of *fait accompli* working in practice.[15]

Finally, deliberate obscurity is a defining characteristic of the ambiguous approach. Although all conflicts are inherently uncertain, gray zone campaigns are designed to be ambiguous in order to disrupt an opponent's strategic calculations and paralyze his decision-making process. Strategic ambiguity is not a new concept; its central aim is to provoke uncertainty in the actions and beliefs (and beliefs about beliefs) of others.[16] The core theme of strategic ambiguity is that one actor is deliberately unclear on a policy in order to balance its interests and to keep all options on the table.[17] The goal is to force the opponent to consider uncertainty about the actor's intentions, capabilities, and possible actions in his strategic calculation. The cost of miscalculation deters the opponent from taking action. US policy toward Taiwan and Israel's nuclear weapons policy are archetypal examples of strategic ambiguity. The use of deliberate obscurity in the ambiguous approach reverses this logic. The aggressor's actions are ambiguous by design in order to hide the source of the threat, the aggressor's intent, or the motivation.[18] The grandmaster of this game is Iran. Critically outmatched in conventional terms, Iran has developed the "Mosaic Doctrine" to confront superior opponents, as it expands warfare beyond the traditional realm to use full-spectrum conflict.[19] Under constant pressure, Iran has realized that its best defense lies "in creating multiple dilemmas for [its] opponents."[20] Strategically innovative use of ambiguity is the crucial factor in keeping a

14 Alexander Lanoszka, "Russian Hybrid Warfare and Extended Deterrence in Eastern Europe," *International Affairs* 92, no. 1 (2016): 189.

15 Steven Metz, "In Ukraine, Russia Reveals Its Mastery of Unrestricted Warfare," *World Politics Review*, April 16, 2014, http://www.worldpoliticsreview.com/articles/13708/in-ukraine-russia-reveals-its-mastery-of-unrestricted-warfare.

16 Stephen Morris and Hyun Song Shin, "Measuring Strategic Uncertainty," July 2002, https://www.researchgate.net/publication/228609097_Measuring_strategic_uncertainty.

17 Brett Benson and Emerson Niou, "Comprehending Strategic Ambiguity: US Policy toward the Taiwan Strait Security Issue," April, 2000, https://www.researchgate.net/profile/Brett_Benson2/publication/229051924_Comprehending_strategic_ambiguity_US_policy_toward_the_Taiwan_Strait_security_issue/links/0f31752fcbf8ac873c000000.pdf.

18 Freier and others, *Outplayed.*

19 Anthony H. Cordesman and Abdullah Toukan, *Analyzing the Impact of Preventive Strikes Against Iran's Nuclear Facilities*, Center for Strategic and International Studies, September 6, 2012, https://csis.org/files/publication/120906_Iran_US_Preventive_Strikes.pdf.

20 Freier and others, *Outplayed.*

conflict under escalation thresholds and delegitimizing the use of military force by an opponent, thus avoiding outright conflict.[21]

Why Conflicts End Up in the Gray Zone

This part of the analysis examines the ambiguous approach as a dependent variable, e.g., as an outcome of strategic interaction between actors. In order to analyze why contemporary conflicts end up in the gray zone, we need to identify the main incentives for adopting the ambiguous approach and the conditions under which it can endure. The leading incentives to conduct conflicts in the gray area appear to be the lack of power and the lack of legitimacy to use brute force.

Violent conflict has been a part of human life since the beginning of recorded history.[22] While the nature of conflict remains unchanged, the character of conflict has continuously adapted to changes in the strategic environment.[23] Since ancient times, the war in the shadows has been part of the war-peace continuum; it cannot be claimed that gray zone conflict represents a new kind of war.[24] However, the current strategic environment is arguably more conducive to the initiation and continuation of these types of conflict than in the past.

After the Cold War, the United States enjoyed a permissive environment in which there was no bargaining against its power.[25] It strives to maintain its technological supremacy and enlarge its global network of alliances and partnerships in order to preserve their advantage over potential near-peer competitors. However, the economic crisis in 2008 and the inconclusive wars in Iraq and Afghanistan pushed the United States to the verge of being overstretched. In the face of globalization, its power is diffusing, leading to a perception of the relative decline of the United States, as others rise. According to Joseph Nye, however, this perception is inaccurate and misleading; the United States will remain strong enough to shape the future of the world.

---

21 Erik Reichborn-Kjennerud and Patrick Cullen, "What is Hybrid Warfare?" *NUPI Policy Brief* 1 (2016), https://nupi.brage.unit.no/nupi-xmlui/handle/11250/2380867.

22 Henry Kissinger, *World Order: Reflections on the Character of Nations and the Course of History* (London: Penguin, 2015), 331.

23 Freier and others, *Outplayed*.

24 International Security Advisory Board, "Report on Gray Zone Conflict," US Department of State, June 30, 2017, https://2009-2017.state.gov/t/avc/isab/266650.htm.

25 Wright, *All Measures Short of War,* 4.

Nevertheless, power is a zero-sum commodity, and even the perception of the decline of status quo power can incentivize revisionists to challenge the existing order, particularly at a regional level.[26] China, Russia, and Iran are actively balancing against the United States. Even though they use the gray zone differently, they have some common characteristics in their behavior. For instance, they are seeking to establish local escalation dominance; they are actively expanding their sphere of influence by targeting weak states, and they are using historical or social connections with targeted states to legitimize their actions.[27] The main effort of revisionist powers is to erode the credibility of the status quo power and test its commitment to provide extended deterrence to its regional allies and partners. If revisionists are successful in changing the equilibrium at a regional level, the liberal world order cannot continue to exist in its present form.[28] Faced with US military supremacy, challengers are forced to find a way to achieve their goals while avoiding direct retaliation from the status quo power. The gray zone allows them to sidestep power asymmetries and re-engage in traditional geopolitical competition.[29]

The vitality of the international order depends on the sensitive balance between power and legitimacy.[30] International law and norms delegitimize the use of force as a way to resolve conflicts. In addition, military forces are not able to score "a decisive victory" in contemporary asymmetric conflicts due to, among other things, the lack of legitimate military targets. As a matter of fact, inconclusive outcomes of military campaigns and the damage inflicted on unintended targets further decrease the legitimacy of using brute force. Most of these conflicts prove the fact that military force is not sufficient to achieve sustainable political objectives. If the status quo power repeatedly exercises power without legitimacy, it strengthens resistance within the system, encourages others to follow the same practice and undermines their authority. On the other hand, if revisionist powers can use military force without punishments, the credibility of both the international system and the status quo power is challenged. Ambiguous conflicts deliberately blur

26 Lawrence Freedman, "A Subversive on a Hill," *National Interest*, no. 101 (2009): 46.
27 Lanoszka, "Russian Hybrid Warfare."
28 Wright, *All Measures Short of War*, 34.
29 Wirtz, "Life in the Gray Zone," 111.
30 Kissinger, *World Order*, 66.

distinctions between legal and illegal actions and allow actors to continue competition without provoking a direct military conflict.

Nevertheless, it is not just revisionists for whom the lack of legitimacy to use force provides incentives to play in the gray zone. Israel is a regional status quo power, with an overwhelming military superiority in the region. However, its ability to use force is limited by its weak legitimacy. Faced with unique hybrid threats and constant accusations of excessive use of force, Israel has no choice but to fight its opponents in the gray zone. Its "campaign between wars" doctrine aims to extend the time between wars by continually working to weaken its opponents and reduce their ability to strengthen themselves; generate optimal conditions for the next war; and build legitimacy for Israeli actions while reducing the enemy's legitimacy.[31]

At the global level, the United States has considerable experience as a significant player in conflicts short of war.[32] From the point of seizing control of the Panama Canal Zone to the end of the Cold War, the United States has proved itself a fierce competitor in this kind of game. However, after the victory in the Cold War, the United States seemed to lose interest in gray area activities at the strategic level. As an unrivaled superpower, the unilateral use of military force was a simple way to pursue US interests. However, unilateral military interventions have damaged US legitimacy and have given challengers an excuse to follow similar practices at the regional level. It is essential for the United States, as the global status quo power, to strike the right balance between power and legitimacy because it has a vested interest in keeping the liberal global order in robust health.[33] In order to restore confidence in the US-led world order, Washington needs to reassure its regional allies and partners that it will protect them from ambiguous threats.[34] At the same time, some authors advocate that the United States should rely more on its power to coerce revisionists without triggering an overt armed conflict. As the most promising measures short of war, they suggested financial and trade sanctions, military embargoes, energy-market

31 "Deterring Terror: How Israel Confronts the Next Generation of Threats," Belfer Center Special Report (Cambridge: Belfer Center for Science and International Affairs, 2016), originally published in Hebrew as the Official Strategy of the Israel Defense Forces.

32 Freier and others, *Outplayed.*

33 Wright, *All Measures Short of War,* 188.

34 Wright, *All Measures Short of War*, 197.

manipulation, offensive cyber activities, exerting sea control, and providing support for political opposition in hostile states.[35]

Current Strategic Environment

A profound understanding of the strategic environment is a precondition for getting the strategy right.[36] Current technological, economic, and social conditions create a favorable environment for conflicts short of war.

The most crucial difference in our conception of warfare is the destructive potential of nuclear weapons.[37] As total war is not a rational option anymore, state actors exploit other alternatives, such as limited conventional war, sub-conventional war, use of force without war, and the threat of the use of force.[38] However, none of these options can entirely exclude the risk of unintended escalation to nuclear confrontation. The United States imposes comprehensive measures, including arms and technology embargoes to prevent the proliferation of weapons of mass destruction and deny antagonistic states access to advanced military technology. On the contrary, emerging and resurgent global powers mitigate the risk of uncontrollable escalation of ambiguous conflicts by emphasizing their willingness to use nuclear weapons to defend their interests.[39] Besides, powers pursuing regional primacy seek to develop nuclear weapons and delivery means as the way to protect themselves from the military intervention of status quo power.[40]

In the age of the fourth technological revolution, the status quo power has to keep its leading position in the race for hi-tech supremacy. Challengers seek to bridge the technological gap by acquiring "game-changing" weapons, such as ballistic and precision strike capabilities, anti-access/area denial (A2AD) systems, anti-satellite weapons (ASAT), directed energy weapons, and kinetic anti-satellite weapons. Although the non-kinetic dimension is predominant in ambiguous conflicts, credible military power has a significant role for both the status quo and revisionist powers. Challengers have to achieve local

35 David C. Gompert and Hans Binnendijk, "The Power to Coerce, Countering Adversaries Without Going to War," (Santa Monica: RAND Corporation, 2016), https://doi.org/10.7249/RR1000.

36 Timothy L. Thomas, "China's Concept of Military Strategy," *Parameters* 44, no. 4 (2014): 42.

37 Schelling, *Arms and Influence*, 21.

38 Jasjit Singh, "Dynamics of Limited War," *Strategic Analysis* 24, no. 7 (2000):1208.

39 Andrew Monaghan, "The 'War' in Russia's Hybrid Warfare," *Parameters* 45, no. 4 (2015): 69.

40 Scott, "Joint Operating Environment 2035."

military dominance to deter military intervention by the status quo power.[41] On the other hand, the status quo power has to demonstrate a willingness to use military force to make its influence strategy works.

Advances in information technology enable aggressors to manipulate the risk of uncontrollable escalation, influence public opinion in the targeted state to an unprecedented level, and exploit ungoverned cyberspace. Both the United States and the revisionist powers have dedicated significant attention to influencing an opponent's attitudes, behavior, and decisions through various communication channels. In ambiguous conflicts, the information campaign plays an essential role. It acts as a force multiplier for other measures short of war.[42] The status quo power has a global media network, enabling the United States to distribute its narrative in order to mobilize allies and isolate opponents. The revisionist powers, on the other hand, take a different approach. They invest substantial efforts and resources in confusing, distracting, dividing, and demoralizing their opponents while shielding themselves from outside information.[43] Their goal is to erode information dominance and deter the status quo power's intervention by delegitimizing the use of brute force. It allows them to engage in "narrative wars" with the status quo power.

The United States has a considerable structural advantage in the cyber domain.[44] As a cyber superpower, the United States has the unparallel ability to monitor, defend, and conduct offensive activities in cyberspace; however, all-out cyberwar is not an option for the United States because it would be no winner.[45] It is the utmost US interest to keep the internet free and open. China and Russia have not been satisfied with the dominant US role in the cyber domain. They have taken different approaches to counterbalance the American advantage in cyberspace. Russia has developed a national internet infrastructure capable of isolating itself from the exchange of external traffic. China, on the other hand, has adopted a set of technological and legislative measures, known as the Great Firewall of China, to internally regulate access to the internet. Both the status quo and revisionist powers are exploring the possibilities of offensive cyber activities as a way to exploit the vulnerabilities

41 Lanoszka, "Russian Hybrid Warfare," 189.
42 Rod Thornton, "The Changing Nature of Modern Warfare: Responding to Russian Information Warfare," *RUSI Journal* 160, no. 4 (2015): 40.
43 Scott, "Joint Operating Environment 2035."
44 Wright, *All Measures Short of War,* 147.
45 Gompert and Binnendijk, "The Power to Coerce."

of increasingly computer-dependent opponents. Cyberspace provides a cost-effective opportunity for launching anonymous offensive operations such as espionage, sabotage, and subversion.[46] Non-attribution is a crucial feature of clandestine activities in cyberspace. It offers the perpetrators the plausible deniability that is crucial for avoiding retaliation. Even though anonymity is useful for bypassing red lines, it can be a disadvantage because coercion requires attribution. In order to achieve political objectives, cyber activities must be integrated with other measures short of war and underpinned by a single strategic rationale.[47]

Economic globalization has created a complex interdependent environment that encourages actors to use economic and financial tools for coercive purposes. Western institutions have regulated global trade and finance since the end of the Second World War, and the US dollar is the world's reserve currency. That enables the status quo power to use economic and financial measures such as market manipulation, trade wars, and sanctions as a means of applying geopolitical pressure. The effects of the US-imposed economic and political sanctions on revisionists depend on the ability of Washington to convince others to respect those sanctions. Coordination with other countries sometimes can be a slow and complicated process. It has been demonstrated that revisionist powers devote significant efforts on driving a wedge between the United States and their allies and partners to mitigate the effects of sanctions. Besides, globalization has increased the level of economic interdependence among nations to an extraordinary level. Wright observed that interdependence restraints aggressors and, at the same time, limits the available responses to their behavior.[48] Imposing financial and trade sanctions on China would be difficult to implement because Beijing plays a critical role in the world economy. Due to the same reason, a trade war between the United States and China may harm both countries and endanger the stability of the global economy.

The vulnerability of the global economy and the existence of powerful actors with conflicting interests increases the opportunity for hostile interactions.[49]

---

46 Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012): 27.

47 Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *Quarterly Journal: International Security* 38, no. 2 (2013): 57.

48 Wright, *All Measures Short of War,* 143.

49 Jeffry A. Frieden, David A. Lake, and Kenneth A. Schultz, *World Politics: Interests, Interactions, Institutions* (New York: W. W. Norton, 2009), 529.

Revisionists are developing their own set of economic instruments for coercion of opponents and as deterrence against status quo power sanctions.[50] Financial deregulation and the 2008 global economic crisis have resulted in a crisis of confidence in the Western economic model. That provides emerging economic powers with the opportunity to promote alternative institutions such as the Asian Infrastructure Investment Bank.[51] Also, China is actively encouraging the renminbi as a regional alternative to the dollar, reducing the potential for the United States to use the dollar as an instrument of pressure.[52] Beijing offers investment in foreign markets without political preconditions, which are very attractive to many countries. As a result, these overseas investments are increasing Chinese global influence.

Socially, the rising impact of public opinion on political decision making provides additional motivation to use the ambiguous approach. The near real-time information environment makes the domestic audience direct participants in expeditionary military conflicts. Western societies have developed unrealistic expectations of a conflict. Public demand for almost zero casualties and strict respect for human rights lead to increasingly complex rules of engagement. At the same time, the constant media presence produces additional pressure. The long "war on terror" and the costly and inconclusive interventions in Iraq, Afghanistan, and Libya have shaken the confidence of Western publics and have undermined their willingness to support expeditionary wars. Under the circumstances, the United States could integrate non-military and military activities in an effort to regain the initiative in the gray zone. However, strategic culture influences the way actors interact in conflict situations. The United States has enormous potential to compete in the gray zone; however, since certain aspects of American strategic culture are unsuited to ambiguous conflict, it has tended only to use measures short of war at the tactical level.[53] Steven Metz observes that the United States prefers situations without political ambiguity where it can use its ultimate military power with the support of its allies.

---

50 Wright, *All Measures Short of War,* 145.

51 John Baylis, Steve Smith, and Patricia Owens, eds., *The Globalization of World Politics: An Introduction to International Relations*, 6th edition (Oxford and New York: Oxford University Press, 2013), 525.

52 Wright, *All Measures Short of War,* 145

53 Connable, Campbell, and Madden, "Stretching and Exploiting Thresholds for High-Order War."

In contrast, Chinese and Iranian strategic culture advocates avoiding unneeded decisive military conflicts.[54] Whenever possible, they instead would take a more sophisticated, indirect approach. Finally, Russian strategic culture has a long tradition of subversive activities and an established record of coordinating and executing subversive activities at the strategic level.[55] In sum, the strategic cultures of China, Russia, and Iran provide solid bases for developing ambiguous approaches to conflicts in the gray area.

Manipulation of Opponent's Risk Perception

Obscurity by design is the distinguishing feature of the ambiguous approach. The competition below the military conflict is a multifaced game that creates as many enigmas for the opponent as possible.[56] Actors can generate ambiguity around four essential elements of conflict interaction: (1) the players involved in the conflict, (2) their actions, (3) the possible outcomes, and (4) the information available to the players.

Ambiguity about the players is designed to conceal the source of the threat. The ability of an aggressor to hide his identity or deny involvement is a crucial part of the ambiguous approach.[57] If a belligerent player can stay hidden, the targeted side has no target at which to retaliate. Furthermore, the unidentified aggressor is likely to avoid punishment or sanctions from the status quo power for breaking international norms and rules. Actors can obscure their participation in conflict through the employment of proxies, use of civilian agencies or groups, or covert operations, including offensive cyber activities. In some cases, it is sufficient for the attacker to hide his identity long enough to present a *fait accompli* to the targeted side. Similarly, the extent of plausible deniability required by the aggressor depends on the particular context. Sometimes, the lack of clarity about the perpetrator is essential to allow the opponent to save face.

Creating ambiguity about the attacker's actions has a twofold aim: sidestepping a defender's established red line commitments and making it difficult to identify, attribute, or publicly define the attacker's actions as the

54 Mazarr, *Mastering the Gray Zone*.

55 Randal G. Bowdish, "Military Strategy: Theory and Concepts," (PhD diss., University of Nebraska—Lincoln, 2013), http://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1026&context=poliscitheses.

56 Mazarr, *Mastering the Gray Zone*.

57 Frans-Paul van der Putten, Minke Meijnders, and Jan Rood, *Deterrence as a Security Concept against Non-Traditional Threats* (The Hague: Cingendael, 2015).

coercive use of force. The ambiguous approach is designed to attack the opponent's deterrence strategy.[58] The fundamental mechanism of deterrence is the manipulation of an opponent's cost-risk calculation.[59] That requires establishing thresholds for military responses. These thresholds do not exist in objective reality but in the minds of decision-makers.[60] As a result, the center of gravity of an ambiguous campaign has to be in the information and psychological domain. Aggressors have two principal options to bypass the opponent's red lines. First, they can stretch thresholds by incrementally testing an opponent's commitment, moving on too small a scale to provoke a reaction.[61] The logic is straightforward: If the attacker meets resistance, he can pretend the action was unintended or unauthorized; if the defender fails to enforce the threshold, then the threshold has been stretched and the aggressor can move to the next step.[62] The aim is to erode an opponent's deterrence while avoiding violently crossing their red lines. The second option is to exploit any weakness in the threshold, such as playing on an opponent's unwillingness to use brute force or taking advantage of an opponent's miscalculation of the threshold.[63] However, this approach can only be used on occasions when the red line suffers from a weakness such as arbitrariness, imprecision, unverifiability, or incompleteness.[64] Exploiting these thresholds requires a profound understanding of their weaknesses. As Iran has successfully demonstrated in Iraq, it is possible to combine stretching the threshold and exploiting the red line in pursuit of strategic objectives.[65]

Another principal aim of creating ambiguity about an attacker's actions is to make it harder to categorize their intentions as confrontational and coercive. This sort of ambiguity can be most effectively generated when the full spectrum of measures short of war is integrated and harnessed

58 Wirtz, "Life in the Gray Zone," 107.
59 Van der Putten, Meijnders, and Rood, *Deterrence as a Security Concept.*
60 Forrest E. Morgan and others, *Dangerous Thresholds: Managing Escalation in the 21st Century* (Santa Monica: RAND Corporation, 2008), 11.
61 Connable, Campbell, and Madden, "Stretching and Exploiting Thresholds for High-Order War."
62 Schelling, *Arms and Influence*, 67–69.
63 Connable, Campbell, and Madden, "Stretching and Exploiting Thresholds for High-Order War."
64 Daniel W. Altman, "Red Lines and Faits Accomplis in Interstate Coercion and Crisis," (PhD diss., Massachusetts Institute of Technology, 2015), https://dspace.mit.edu/bitstream/handle/1721.1/99775/927329080-MIT.pdf?sequence=1.
65 Connable, Campbell, and Madden, "Stretching and Exploiting Thresholds for High-Order War."

under a single strategic rationale. Actors with more centralized power are usually more successful in integrating all the instruments of national power in conflicts short of traditional war.[66] Effective coordination of measures short of war allows the belligerent to orchestrate activities across different domains (non-military and military), thus obscuring its actions and intentions and reducing the risk of violent retaliation.

A vertical escalation, similar to that in traditional wars, involves an increase in the intensity of activities.[67] However, it should be emphasized that vertical escalation in ambiguous conflicts is not designed to cross over the "culminating point of coercion."[68] On the other hand, a horizontal escalation in ambiguous conflicts involves synchronizing the effects of both military and non-military elements of national power.[69] Given that the opponent's perception is the center of gravity of the ambiguous approach, the informational domain plays the most dominant role. The ambiguous approach uses all dimensions of conflict escalation in the gray zone, cautiously testing the opponent's commitments and exploiting threshold vulnerabilities to generate the desired strategic effect. Kahn defined the combination of vertical and horizontal escalation as "compounding escalation."[70]

The possibility of an unintended escalation of a gray area conflict into a full-scale war is always present, particularly considering that the aggressor has to contain the conflict geographically while preventing external intervention. However, if a targeted state is ready to incur the risk of military confrontation, the aggressor will struggle to maintain escalation control regardless of his local military dominance.[71]

The next area where actors can deliberately create ambiguity is the set of possible outcomes. Well-designed ambiguous action should allow the opponent to ignore the outcome of an actor's action either because the adversary wants to "save face" or because he is not aware of a particular outcome. Also, an actor can use the fact that payoffs attached to an opponent's outcomes may be

66 Rod Thornton, "The Changing Nature of Modern Warfare: Responding to Russian Information Warfare," *RUSI Journal* 160, no. 4 (2015): 40–48.
67 Morgan and others, *Dangerous Thresholds*.
68 Dmitry (Dima) Adamsky, "From Moscow with Coercion: Russian Deterrence Theory and Strategic Culture," *Journal of Strategic Studies* 41, no. 1–2 (2018): 56.
69 Reichborn-Kjennerud and Cullen, "What is Hybrid Warfare?"
70 Herman Kahn, *On Escalation: Metaphors and Scenarios* (New Brunswick: Routledge, 2009), 4–6.
71 Jan Angstrom and Magnus Petersson, "Weak Party Escalation: An Underestimated Strategy for Small States?" *Journal Of Strategic Studies* 42, no. 2 (2019): 282–300.

multidimensional, but this requires a deep understanding of the adversary's strategic culture. In that case, the cross-domain coercive campaign could influence an adversary's will and choices and avoid unintended escalation. As a rule, ambiguous actions expand the set of possible outcomes in conflict. An actor can hide his desired outcome or avoid exposing the limits of his intentions. In either case, the aim is to complicate the opponent's strategic calculations.

The ability to shape the adversary's perception of the strategic environment is the critical factor in conflict in the gray area: Ambiguous information influences opponent's assertiveness and responsiveness. A lack of clarity over the facts creates profound risk-confusion for the opponent and disrupts their strategic calculations.[72] When decision-makers face an ambiguous threat, they tend to "ignore and discount the risk and take a wait-and-see attitude."[73] Even if they are aware of the nature of the threat, their lack of clarity over the aggressor's risk threshold and fear of escalating the conflict may lead them to choose inaction over action. Decision-paralysis in the face of ambiguous information is likely to be fatal from a strategic perspective.

Depending on the broader context and specific circumstances, the ambiguous approach may be designed to create confusion about one or more elements mentioned above.

Conclusion

Campaigns in this gray area follow the logic of the ambiguous approach. This essay argues that the ambiguous approach is based on three essential elements. First, it requires the synchronization and coordination of all available measures short of war at the strategic level, and second, the employment of coercive gradualism against the interests of other nations. Finally, conflicts in the gray area are intentionally designed to be ambiguous.

The asymmetry of power between the United States and near-peer competitors, combined with the decreased legitimacy of using brute force in international relations, provides significant incentives for actors to move the conflict into the gray area. At the same time, actors' ability to operate in the gray zone is enhanced by technological advances, economic globalization, and current social conditions.

72 Freier and others, *Outplayed*.

73 Michael Roberto, Richard M. J. Bohmer, and Amy C. Edmondson, "Facing Ambiguous Threats," *Harvard Business Review*, November 1, 2006.

A deliberate ambiguity may be created around participants in the conflict, their actions, possible outcomes, and information available to the opponent. The cumulative effect of this intentional ambiguity is a disruption of the opponent's decision-making process, providing opportunities for an actor to stretch or exploit opponent's red lines and to avoid attribution and crossing the threshold of military response.

An ambiguous approach allows actors to shape their opponent's risk perception and risk appetite. However, conflict in the gray area, like any other conflict, remains dialectic of opposing wills that can trigger uncontrollable escalation to all-out war or other unintended consequences. It can be a result of miscalculation or rational strategic choice of one side to escalate conflict out of the gray zone.

Cybersecurity and Information Security: Force Structure Modernizations in the Chinese People's Liberation Army

Miranda Bass

Since 2012, the Chinese government under Chairman Xi Jinping has taken steps to assume the role of a global power, including a sweeping modernizing of its military, the People's Liberation Army (PLA), in order to transform it into a force capable of projecting power. Notably, in 2015, the PLA formed the Strategic Support Force as a separate service, concentrating all of its satellite and network operations forces, including cyber operations forces, into a single, high-profile organization. This policy choice to reorganize the PLA force structure reflects and reinforces the new preeminence of information operations in China's national security, the majority of which takes place in cyberspace.

Keywords: China, military, cyber, force structure, modernization, information operations, national security

Introduction

All militaries need to evolve commensurately with developments in military technology and the strategic and political goals of their society. The Chinese People's Liberation Army (PLA) was born as the military wing of the Chinese Communist Party (CCP). It has remained an army of the party ever since and has not transitioned into a national military. It began its first efforts at modernization under Chairman Deng Xiaoping in 1979 with the whole-of-society Reform and Opening movement and following a painful loss in the

First Lieutenant Miranda Bass, US Army is an MA candidate at Tel Aviv University.

Sino-Vietnamese War. As China has assumed a powerful global role over the past twenty years, the PLA has sought to expand beyond being a low-capacity, internally focused conscript army to becoming a formidable regional force. Both the goals of advancing global status and military modernization, nested therein, have accelerated under Chairman Xi Jinping since he took office in 2012. An integral part of the orientation and capabilities of a military is its force structure, which also evolves with modernization efforts. Force structure is a fundamental aspect of the composition of a military and a challenging area in which to introduce new systems due to bureaucratic resistance. Thus, any developments in this area are the result of long-term, high-level commitment and dedicated effort. Beginning in the early 2000s and particularly over the last five years, the PLA and Chinese government as a whole have taken major steps to codify and institute comprehensive cyber policy, culminating in a gargantuan modernization of its military force structure in 2015, including a total reorganization of PLA forces involved in cyber operations. The main thrust of this reorganization was the formation of the Strategic Support Force (SSF) 解放军战略支援部队 *jiefangjun zhanlue zhiyuanbudui* on December 31, 2015. This paper will detail the changes within the PLA and explain how the establishment of the SSF was a sound decision for China's goals in cyberspace and information management.

Cyberspace, Cyberattacks, and Cyber Defense

Cyberspace is a notoriously difficult term to pin down due to its manifold use in contemporary discourse. While the popular notion of a link between cyberspace and electronics is true, it is not the whole story. From a security perspective, a useful definition of cyberspace comes from its components, three layers resting one on top of the other: physical, syntactic, and semantic.[1] Every layer is necessary for cyberspace to exist as a whole and without one, the whole system would disappear, albeit perhaps only temporarily. The physical layer of cyberspace consists of the medium's tangible infrastructure, including wires and boxes filled with electronics that physically sit in various sites around the world. From a security perspective, the salience of the physical layer is the potential for an adversary to attack these boxes and cripple the ability of people and machines to operate in cyberspace.

1 Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND Corporation, 2009), 39.

The syntactic layer is unseen, occupied by the machines and protocols that facilitate all exchanges and operations in cyberspace. This layer is the domain of machine interaction, including routing and switching. Most hacking, which is a cyberspace interaction in which one party completes an action for its own benefit through the perversion of existing pathways to the detriment of other parties, takes place at the syntactic level. The semantic layer contains the vast majority of the data and interfaces that the typical user commonly conceives of as cyberspace in that it exists separately, although often adjacently, to the natural world. Unlike the syntactic layer, the semantic layer appears mostly in natural human language.

With a working definition of cyberspace, it is possible to turn to hacking, the twisting of the medium's intended pathways for human ends. The typical goal of hacking is to steal data, usually from another user or system's machine.[2] In security terms, these cyber activities are known as computer network exploitation (CNE) and can happen between any type of actor. A state may, and they often do, steal data from another state, organization, or individual to advance its national goals; corporations steal intellectual property from each other; and individuals steal data from any entity to commit identity theft, for ideological motivations, or for any other potential goal a person might have. It is worth having a basic understanding of the general outline of CNE in order to discuss its ramifications in government and military force structure. Stealing data is non-rivalrous, meaning that its theft does not impede its free use unlike stealing an object like rocket launchers, and anyone or anything monitoring the system hosting the data may not realize that theft has even taken place.[3] CNE begins with the exploiting party obtaining unauthorized access of the target system, receiving the privileges, the level of access, of a user or administrator in that system. The exploiter then attempts to pilfer the desired data while evading detection to enable the highest chance of success. Due to the non-rivalrous nature of CNE, this outcome is entirely possible.

Fundamentally, CNE is espionage, which states traditionally have not considered an act of war prior to the rise of cyberspace. CNE does not deprive the user of full use of the machine; the user suffers no harm apart from losing information; and the law of war does not recognize espionage as *casus belli*, a cause sufficient to initiate a war.[4] A cyberattack often looks similar to CNE

2 Libicki, *Cyberdeterrence*, 14.
3 Libicki, *Cyberdeterrence*, 15.
4 Libicki, *Cyberdeterrence*, 23–24.

in its early stages, due to the realities of operating in cyberspace, but it has a different goal. A cyberattack is the deliberate disruption or corruption by an attacker, usually a state, of a target system of interest to another state. Similarly to CNE, after the attacking party gains the required privileges, it then proceeds by either disrupting the system so that it does not function properly, causing drastic, obvious, and immediate effects, or corrupting the system in subtle, even unnoticeable ways that may linger or reoccur.[5]

Commensurately to cyberattacks, cyber defense came into existence, albeit of a less thrilling character, as is often relegated to defense in security generally. The goal of cyber defenders is to render their system as impervious as possible to unwanted infiltration of any kind, be it CNE or a cyberattack. System managers can go to great lengths to ensure that a system has a high degree of security, but this outcome is ultimately not ideal for the system's users. The classic problem of security in cyberspace is the tradeoff between security and accessibility. Networked systems exist in order to facilitate user operation and interaction with other machines and the internet. This necessary openness, combined with the original conception and design of the internet as a borderless space largely without security measures, has created a situation in which cyber defenders are at a disadvantage.

States are by no means the only perpetrators of cyberattacks or pursuers of cyber defense, but states that invest heavily in this area are undoubtedly the most sophisticated type of actor due to their size, resources, and goals. National cybersecurity capabilities, encompassing the ability to attack, defend, and conduct espionage, vary widely between states based on the priority that the government has placed on developing this new tool. Although the wealthiest states have bolted ahead in their relative capabilities as with other technological innovations, cyber operations merit a paradigm different from the last major historic innovation in military technology, that of nuclear technology. In contrast to nuclear technological development, which was prohibitively expensive for the vast majority of states and certainly for non-state actors, cyber capabilities are radically accessible to any actor, including private individuals. Due to their immense resources and comparably complex targets, states have the most sophisticated capabilities, but the field is no longer restricted to the wealthiest states; even the poorest states can have

5 Libicki, *Cyberdeterrence*, 15–16.

an outsized effect, like North Korea. Critically, non-state actors can act independently and effectively as well.

Cyberspace is not merely the technological; rather, it is the tool of its users, meaning that any threat comes not from the machines but from the people who design and operate them.[6] Even today cyberspace is still reminiscent of the American West of old, a place vast, unmapped, culturally and legally ambiguous, terse, difficult to navigate, and largely up for grabs.[7] This environment is fertile ground for the innovation about how the world ought to be shaped, which actors and category of actors should be powerful, how communication ought to look, what truth is, and what liberty means. Despite or in conjunction with these possibilities, cyberspace still remains a reflection of the broader, non-cyber world and its power arrangements. Its main contribution to the structure and distribution of power is a lowered barrier to entry for an actor to achieve global relevance, which is no small innovation. In addition to lowered barriers to entry, actors in cyberspace enjoy the near-total irrelevance of spatial distance, net-speeds approaching lightspeed, and a higher degree of difficulty in definitively attributing a particular act to a specific actor. Another less intuitive distinction of cyberspace is that it is nearly impossible to know who will witness a given event, where and when they might see it, or how they might interpret it.[8]

Categories of Cyber Power in National Security

There are several types of cyber power in a national security conception.[9] The broadest is productive cyber power, the construction of discourse in cyberspace, which includes both reinforcing existing discourse and inventing and disseminating something new. Cyberspace uniquely facilitates discourse and its amplification with minimal barriers. Structural cyber power is the maintaining of existing power structures and enabling or constraining actors within these structures. Structural cyber power tends toward the anarchic, in particular enabling eye-catching vitriol and resentment of disaffection to flourish and propagate. Institutional cyber power is the control of cyberspace through institutions such as the Internet Corporation for Assigned Names

6 David J. Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-power* (London: International Institute for Strategic Studies, 2011), 13.
7 Betz and Stevens, *Cyberspace and the State,* 14.
8 Betz and Stevens, *Cyberspace and the State,* 40.
9 All of the following types of cyber power are derived from Betz and Stevens, *Cyberspace and the State,* 45–50.

and Numbers (ICANN), an American non-profit responsible for coordinating databases of names and numerical addresses on the internet. This type of cyber power also extends to informal institutions, namely, norms, which construct and are constructed by actors' behavior in cyberspace. The narrowest form is compulsory cyber power, which includes CNE and attacking to control a machine or network's behavior, preventing an actor from operating in cyberspace and similar operations of coercion.

All these types of cyber power are relevant to the military, which is a key body in a country's national cybersecurity policy and operations, although certainly not the only one. The link to the military of compulsory cyber power is self-evident, as it is often the military that executes such operations. The link to structural cyber power is relevant both in that structural cyber power broadens the threat possibilities, from primarily state actors or only the most highly organized and capable non-state actors to networked individual nodes acting with lowered barriers to entry. In short, cyberspace weakens the constraints of existing power structures with respect to which actors have access to impactful global interactions. Institutional cyber power is relevant to military power in that the norms of military operations in cyberspace are still being written. Thus, a military that seeks to create the rules of the game in its own interests, which is the case in every state that has the capability or aspiration for international influence, seeks to expand its own internal structural cyber power as well as that of its state in general. Productive cyber power is more unique in that it links the military realm of war with its political dimension by enabling an actor to mold discourse to its strategic advantage. Although this activity originates in the political realm, not the military, military organizations can still undertake operations in this line of effort and are indelibly shaped by them.

The traditional Clausewitzian definition of the object of war is the overthrow of one's enemy, rendering the adversary powerless. Based on this understanding, cyber power is a force multiplier, but not a substitute for physical force.[10] However, according to a soft power understanding of war using the model of Joseph Nye, the object of the conflict is persuasion, and cyber power could be strategically decisive in this framework; nonetheless, this definition is not quite as helpful. Cyber power is an increasingly critical complement to other more kinetic capabilities, but it certainly does not negate

10 Betz and Stevens, *Cyberspace and the State*, 86.

these capabilities or change the objective nature of war. What it does do, crucially, is give a weapon to the historically weak, militarily and politically. Over the last several centuries, the West has maintained its military and political power through a virtuous cycle of economic and political expansion. Since decolonization, however, its military power has achieved less effective and decisive results through kinetic action and weapons. To address this, Western states have changed tactics to utilize the allure of ideas, based on Nye's soft power mold, which has been successful.[11] Because of this reality, actors opposed to Western hegemony, particularly, illiberal regimes, now perceive the free internet and all of its discourse and information to be a knife at their throats.[12] Thus, it is a national security imperative for regimes in which authoritarianism and illiberal politics are the order of the day to control the flow of ideas. No major political entity has more thoroughly understood this imperative and acted accordingly than the CCP, in large part because the party developed from a totalitarian system amidst the throes of the twentieth century and has adhered to ideological purity including Marxist discourse control since its inception.

The question of how exactly the CCP has gone about controlling the internet, cyberspace, and information in general is beyond the scope of this paper. For these purposes, however, the CCP describes the potential of the internet as an engine of economic development, a vehicle for more easily creating and disseminating culture, a platform for social governance both by enhancing individual rights and facilitating government control, and a territory that demands national sovereignty just as land, sea, sky, and space do.[13] Beside the benefits, the party identifies the primary threat of cyber penetration to be challenges to Chinese political security, which is foundational to national development and the happiness of the people, by instigating social unrest. Cyberattacks threaten economic security and so-called harmful information threatens the security of traditional culture.[14] What follows is the structure of the PLA's cyber and information operations forces and, crucially, the military modernization project of 2015, how the

11 Betz and Stevens, *Cyberspace and the State*, 132.
12 Betz and Stevens, *Cyberspace and the State*, 132.
13 Office of the Central Cyberspace Affairs Commission, "Guo jia wang luo kong jian an quan zhan lue," *Zhongguo Wangxinwang*, December 27, 2016 (accessed December 10, 2019), http://www.cac.gov.cn/2016-12/27/c_1120195926.htm.
14 Office of the Central Cyberspace Affairs Commission, "Guo jia wang luo kong jian an quan zhan lue."

modernization has reshaped those same forces, and why the change in force structure supports the party's military goals.

Before discussing technical military organization, it is necessary to understand the Chinese conception of cybersecurity, which, like so much Chinese thought, is different from the common Western understanding. The Western idea of cybersecurity in China is called network security 网络安全 *wangluo anquan*. This idea fits under the umbrella of the broader idea in China of information security 信息安全 *xinxi anquan*, which is more about content management; that is, censorship and control of information dissemination is the object of the semantic layer of cyberspace rather than network security or integrity *per se*.[15] A former chair of the organization that produced China's first cybersecurity policy document argued that information security was "necessary for social stability and socialist cultural and ideological development."[16] These words are not empty rhetoric. They are foundational to the CCP's national security concept and, in particular, its cybersecurity concept.

Informationization in the PLA

"Informationization" is the most accurate translation of the Chinese term 信息化 *xinxihua*, a guiding principle of the PLA's modernization and transformation from an internally oriented farmer's army into a power projector. To the extent that there is any civil society in China at all, it exists on the internet.[17] This poses a potentially critical threat to stability in China, which, according to the CCP, is based on the total absence of any discernable dissent or dissatisfaction with party rule. Chinese cyber policy began to emerge in the early 2000s from the State Information Leading Group (SILG) and State Council Information Office, two early organizations that worked on information security. The seminal policy piece is a SILG opinion from 2003 referred to as Document 27, which established China's national

15 Jon R. Lindsay, "Introduction—China and Cybersecurity: Controversy and Context," in *China and Cybersecurity: Espionage, Strategy and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (Oxford: Oxford University Press, 2015), 11.

16 Qu Weizhi, *China's Path to Informationization*, cited in Jon R. Lindsay, "Introduction—China and Cybersecurity: Controversy and Context," in *China and Cybersecurity: Espionage, Strategy and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (Oxford: Oxford University Press, 2015), 11.

17 Weizhi, *China's Path to Informationization*, 1.

cybersecurity policy for the first time in exclusively defensive terms.[18] In the following decade, a dense bureaucratic tangle of offices and institutions was responsible for disparate aspects of the creation and management of Chinese cybersecurity policy. Progress during this period was halting, as government attention was diverted to other priorities: first, planning for the 2008 Beijing Olympics and then the global financial crisis. In 2012, however, Chairman Xi took office and the CCP began to move toward increased social control and a less open society and to aspire to become a top global power. Upon taking office, Chairman Xi immediately began to reorganize government offices according to new policy priorities, and in 2014 the SILG became the Cybersecurity and Informatization Leading Group (CILG), which Chairman Xi personally led and continues to lead along with the other highest-ranking party leaders in the country. These staffing decisions raised the issue of military informationization to the highest level of importance in policy. PLA military doctrine is weighted heavily toward the offensive on the operational level, including preemptive strikes, and has a defensive orientation at the strategic-political level.[19] Functionally, this doctrine means that since the PLA cyber forces are engaged in operations short of outright war, they are highly active and aggressive. Cyber operations-specific doctrine emphasizes striking first in an armed conflict with cyberattacks to paralyze the adversary's command and logistics systems.[20]

Pre-Modernization Force Structure

By the first half of this decade, the PLA had developed a large complement of cyber-engaged and cyber-adjacent forces. The PLA General Staff Department (GSD), subordinate only to the supreme command authority (the Central Military Commission), was responsible for day-to-day joint operations, intelligence, strategic planning, operational requirements, training, mobilization, military diplomacy, and the security of senior leaders, making

18 Weizhi, *China's Path to Informationization*, 8.

19 Kevin Pollpeter, "Chinese Writings on Cyberwarfare and Coercion," in *China and Cybersecurity: Espionage, Strategy and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (Oxford: Oxford University Press, 2015), 141.

20 Lindsay, "Introduction," 18.

it the cutting-edge driver of the PLA's future.[21] The GSD contained the 2nd, 3rd, and 4th Departments, notated as 2/PLA, 3/PLA, and 4/PLA, respectively.[22] 2/PLA was China's human intelligence (HUMINT) organization, conducting foreign intelligence collection from human sources. Their overt operations were conducted by a global network of defense attachés, selected for their analytical capabilities and language skills, and typically lacking conventional military experience.[23]

3/PLA was China's signals intelligence (SIGINT) organization which had its origins in pre-internet traditional SIGINT but by the twenty-first century was dealing with all forms of SIGINT. Its mission and operations consisted primarily of cyber reconnaissance and CNE.[24] 4/PLA was far more secretive and conducted more disruptive activities in the fields of electromagnetic warfare, information operations and warfare, and computer network attacks (CNA).[25] The PLA has three categories of cyber military operations, which it terms computer network warfare 计算机网络战 *jisuanji wangluo zhan*: computer network reconnaissance, which is CNE; computer network strike, CNA; and computer network defense (CND).[26] Within computer network warfare, doctrine articulates offensive operations as destroying adversary network systems, information, and degrading adversary operational effectiveness. Defense operations include protecting Chinese network systems, information, and the conduct of operations, essentially the converse of their offensive operations.[27]

3/PLA is of particular interest due to its high-profile cyber operations. It was the largest employer of top-tier linguists in the country in 2014 and engaged in advance computing, encryption, and decryption.[28] Its headquarters were

21 Mark Stokes, "The Chinese People's Liberation Army Computer Network Operations Infrastructure," in *China and Cybersecurity: Espionage, Strategy and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (Oxford: Oxford University Press, 2015), 164.

22 Stokes, "The Chinese People's Liberation Army Computer Network Operations Infrastructure."

23 Nigel Inkster, "The Chinese Intelligence Agencies: Evolution and Empowerment in Cyberspace," in *China and Cybersecurity: Espionage, Strategy and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (Oxford: Oxford University Press, 2015), 33.

24 Inkster, "The Chinese Intelligence Agencies."

25 Inkster, "The Chinese Intelligence Agencies."

26 Pollpeter, "Chinese Writings on Cyberwarfare and Coercion," 143.

27 Pollpeter, "Chinese Writings on Cyberwarfare and Coercion," 139.

28 Stokes, "The Chinese People's Liberation Army Computer Network Operations Infrastructure," 164.

located in the Haidian district of Beijing, close to many of the highest-level government offices. 3/PLA command oversaw a headquarters unit, political department, logistics department, Science and Technology (S&T) Intelligence Bureau, S&T Equipment Bureau, and the 56th Research Institute, the PLA's oldest and largest computer science R&D institution.[29] Also under 3/PLA was the secretive Beijing North Computer Center (BNCC), responsible for cyber reconnaissance architecture design, technology development, systems engineering, and acquisition. BNCC was one of the first PLA organizations responsible for cyber operations in their twentieth-century infancy and contained ten subordinate divisions responsible for computer network operations (CNO), which include the full spectrum of CNE, CNA, and CND.[30] 3/PLA operational personnel and linguists received their training at specialized PLA universities.[31] Other cyber operations assets, termed Technical Reconnaissance Bureaus (TRBs), existed outside of 3/PLA. The three PLA services (PLA Air Force, Navy, and Second Artillery or Strategic Rocket Force) each had their own TRBs, as did each of the seven military regional commands. The PLA Air Force had three regional TRBs that monitored the activity of neighboring air forces, conducted airborne SIGINT missions, and conducted CNO that directly supported air force operations. The PLA Navy had two TRBs, one each for the northern and southern seas, and were likely occupied with ship-based SIGINT collection. 2nd Artillery also had its own TRB. The TRB serving each military regional command supported the command's operations. A detailed account of 3/PLA's operational bureaus and their activities follows addressing exactly in which operations the PLA cyber operational forces were and continue to be engaged.

3/PLA had direct authority over twelve operational bureaus, eight headquartered in Beijing, two in Shanghai, one in Qingdao, and one in Wuhan. These TRBs existed and operated independently of those under the services and military regional commands. 3/PLA also had a dedicated Hong Kong and Macao office.[32] The unit commander had a corps-level grade, and

29 Stokes, "The Chinese People's Liberation Army Computer Network Operations Infrastructure," 166–167.

30 Stokes, "The Chinese People's Liberation Army Computer Network Operations Infrastructure," 168.

31 Stokes, "The Chinese People's Liberation Army Computer Network Operations Infrastructure," 169.

32 This and all bureau information is taken from Stokes, "The Chinese People's Liberation Army Computer Network Operations Infrastructure," 170–172.

the bureau directors and their equally powerful political commissars had division-level grades, overseeing between six and fourteen offices. First Bureau, headquartered in Haidian with 3/PLA headquarters, was one of the foremost national authorities on CNO and information security. Second Bureau, primarily in Shanghai, targeted the United States and Canada in pursuit of political, economic, and military intelligence while also maintaining professional affiliations and research relationships with numerous academic institutions in the area. Third Bureau, headquartered in Beijing, had at least thirteen geographically dispersed subordinate units, indicating that the Third Bureau was likely occupied with collecting from line-of-sight radio, direction finding, and emission control and security. Fourth Bureau was headquartered in Qingdao, a port city, and focused on Japan and the Korean Peninsula, with offices up and down the coast. Fifth Bureau was also headquartered in Beijing, with offices in Heilongjiang, one of the northernmost provinces of China, and had a Russia mission. Sixth Bureau was headquartered in Wuhan, in central China, and had offices spread across the whole region, indicating a Taiwan and South Asia mission. Seventh Bureau was also headquartered in Haidian and employed some English translators. It participated in CNO, but its mission was unclear. Eighth Bureau was adjacent to 3/PLA headquarters and focused on Europe and perhaps the Middle East and Latin America as well. Ninth Bureau was the most opaque, headquartered just outside Beijing, and was responsible for computing, analysis of strategic intelligence, database management, and audiovisual technology. Tenth Bureau was headquartered in Beijing and had a Central Asia or Russia mission, perhaps specifically in the fields of telemetry, missile tracking, and nuclear testing. Eleventh Bureau was also headquartered in Beijing and had a Russia mission. Twelfth Bureau was headquartered in Shanghai and had a satellite mission, focused on space-based SIGINT.

3/PLA had the lead role in CNE and CND, but the lead CNA organization was likely the more secretive 4/PLA, which held the formal name of the Electronic Countermeasures and Radar Department. 4/PLA was responsible for radar joint operational requirements development and electronic countermeasures (ECM), including satellite jamming and counter-stealth radar systems.[33] The organization included at least four bureaus, an advisory group, and the 54th

33 Stokes, "The Chinese People's Liberation Army Computer Network Operations Infrastructure," 174.

Research Institute. The ECM Bureau planned, programmed, and budgeted for ECM systems; the Technical Equipment Bureau was occupied by acquisition; and personnel assigned to 4/PLA received specialized training in a dedicated PLA university. There were at least two known operational ECM brigades, and they were likely responsible for electronic reconnaissance satellite ground receiving stations that supported joint targeting as well as satellite jamming.

Post-Modernization Force Structure

All of these organizations were transformed, however, with a decision that took effect on January 1, 2016. Instead of the numerous, more dispersed organizations operating underneath the GSD, all cyber and information operations assets were placed under the Strategic Support Force (SSF) as part of a general force-structure overhaul. The seven military regional commands were reorganized into five theater commands, and the new theaters were awarded the command authority that formerly belonged to the individual services in order to better facilitate joint operations like most expeditionary militaries.[34] This force structure reorganization removed TRBs that had been directly subordinate to the services and military regions and placed them under the authority of the SSF. The SSF is the PLA's fully integrated joint information warfare force, providing the PLA with strategic information using primarily network-based and space-based capabilities, and these are its two primary departments.[35] These capabilities include communications, navigation and positioning, intelligence, surveillance and reconnaissance, and protecting PLA information infrastructure.[36] The SSF conducts information operations in space and cyberspace, electronic warfare, and psychological operations. Thus, by nature it is not a dedicated cyber operations force, but, rather, a dedicated information operations force that operates primarily in cyberspace as well as other mediums, commensurate with the Chinese understanding of information security and cyberspace. The GSD and other

34 Xinhua News, "Xin shi dai de zhong guo guo fang," *Xinhuanet*, July 24, 2019 (accessed December 10, 2019), http://www.xinhuanet.com/politics/2019-07/24/c_1124792450.htm.

35 Adam Ni and Bates Gill, "The People's Liberation Army Strategic Support Force: Update 2019," *Jamestown Foundation China Brief*, May 29, 2019 (accessed October 9, 2019), https://jamestown.org/program/the-peoples-liberation-army-strategic-support-force-update-2019/.

36 Ni and Gill, "The People's Liberation Army Strategic Support Force."

organizations housing forces that had similar mission sets were all disbanded at the end of 2015.

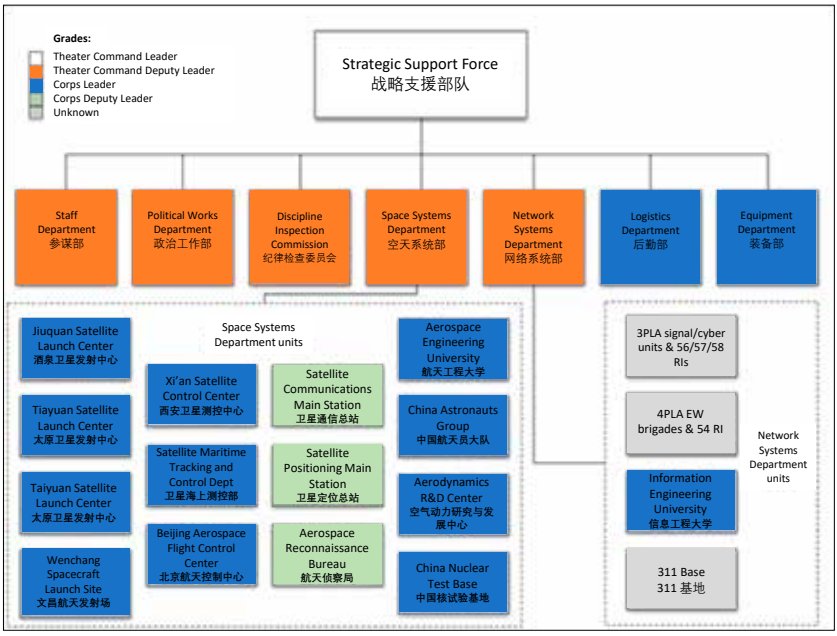

Figure 1. The Strategic Support Source

Source: Adam Ni and Bates Gill, "The People's Liberation Army Strategic Support Force: Update 2019," *Jamestown Foundation China Brief*, May 29, 2019 (accessed October 9, 2019), https://jamestown.org/program/the-peoples-liberation-army-strategic-support-force-update-2019/.

In addition to the two operational Space Systems and Network Systems Departments (SSD and NSD respectively), the SSF also has a staff department responsible for operations, planning, training, project management and oversight, and personnel management.[37] The political works department is an integral part of any PLA body. In this army, being of the party and not the nation as a whole, every organization must maintain integrity of political thought and mission in line with party ideology. The SSD handles nearly every aspect of the country's space operations and the NSD subsumed the former 3/PLA and 4/PLA network missions, including SIGINT, cyber espionage, CNO, electronic warfare, and psychological operations. Thus, the new force does not conduct significantly different operations from what 3/

37 Ni and Gill, "The People's Liberation Army Strategic Support Force."

PLA and 4/PLA have been doing for years, but it has been raised to the level of a full-fledged PLA service, comparable to the 2nd Artillery, indicating the elevation of the status of information operations to the highest level.

Chinese language sources reinforce with exactingly particular rhetoric in official discourse that the SSF is a new type of war-fighting power 新型作战力量 *xinxing zuozhan liliang*, which means that the CCP considers the SSF and information operations to be a veritable domain for national security.[38] Official sources report that SSF information operations and the creation of such a force are representative of Military Modernization with Chinese Characteristics 中国特色强军 *zhongguo tese qiangjun*, a phrase that echoes the decades-old refrain of Socialism with Chinese Characteristics 中国特色社会主义 *zhongguo tese shuhuizhuyi*, which was and continues to be a guiding principle for national Reform and Opening 改革开放 *gaige kaifang*. Official sources describe the SSF as helping to achieve the Chinese Dream and the dream of military modernization, and that all officers and soldiers must adapt to the new policies.[39] The entire structure of the PLA, not just the creation of the SSF, is undergoing modernization in order to improve national security, while the SSF, in particular, is a new war-fighting power in national defense.[40]

Conclusion

The restructuring of cyber forces inside the PLA is part of the modernization project of the entire military that began in 2015. China's defense white paper of 2019 identifies its two goals for 2020 to be mechanization, which is the physical modernization of tactical equipment, and informationization construction, which refers to institutions within the PLA that manage information security and, nested therein, cyber security.[41] By 2035, the PLA's stated goal is to fully complete military modernization and to operate in

38 Liu Shangjing ed., "Guo fang bu zin wen fa xin ren jiu shen hua guo fang he jun dui gai ge you guan wen ti jie shou mei ti zhuan fang," Ministry of National Defense of the People's Republic of China, January 1, 2016 (accessed October 9, 2019), http://www.mod.gov.cn/info/2016-01/01/content_4637926.htm.

39 Xinhua News, "Lu jun ling dao ji gou huo jian jun zhan lve zhi yuan bu dui cheng li da hui zai jing ju xing xi jin ping xiang zhong guo ren min jie fang jun lu jun huo jian jun zhan lve zhi yuan bu dui zhi xu jun qi bing zhi xun ci," *Xinhuanet*, January 1, 2016 (accessed October 9, 2019), http://www.xinhuanet.com//politics/2016-01/01/c_1117646667.htm.

40 Xinhua News, "Lu jun ling dao."

41 Xinhua News, "Lu jun ling dao."

the same league as the world's leading militaries. This larger goal includes modernization of military theory, organizational forms or force structure, weapons, and equipment.[42] Standing up the SSF is the fruition of the goal of informationization construction, and it will likely remain the primary force structure for PLA cyber operations forces in the coming decade. As stated in their white paper, more force structure changes may occur before 2035 in order to complete the modernization project. With the SSF as the new organizational form for cyber operations forces, however, future modernizations are unlikely to dramatically alter this force structure; rather, major force structure changes are more likely to alter the precise chain of command under which the SSF falls and not the organization itself.

The sweeping 2016 force structure reorganization creating the SSF may have produced few changes on an operational level for the former 3/PLA and 4/PLA mission sets beside elevating their status. Nonetheless, it represents and reflects a change of the highest order in military strategy and priorities in which information operations have become a new domain of warfare that is absolutely critical to the continued domestic peace that the CCP requires in order to maintain its authority and legitimacy as the only game in town that can keep such a populous and physically vast country tranquil and prosperous. To this end, the CCP under Chairman Xi's highly centralized and effective leadership took cyber operations from bureaucratic confusion and backwaters, and formed it anew under the umbrella of information operations, so that the mission most directly supported the CCP goals of ideological unity and intolerance of dissent as ways to realizing national security. The force structure reorganization was a reflection of and an effective enhancement for new cybersecurity and information security policy, as the Chinese understand that the two come hand in hand.

42 Xinhua News, "Xin shi dai de zhong guo guo fang."

Chinese investments in Sri Lanka: Implications for Israel

Shlomi Yass

This article addresses Chinese projects in Sri Lanka, some of which are within the Belt and Road Initiative, in order to draw insights to be applied to the Israeli sphere. Moreover, the article will try to answer whether, and to what extent, the Chinese Belt and Road Initiative "belongs to the world," as is written on its official website, or whether this is an expression of the Chinese drive for influence that may lead to a new Chinese world order.[1] The article presents the Belt and Road Initiative alongside arguments against it. It then outlines Chinese-Sri Lankan relations and lists four Chinese projects on the island. The article then examines Israel-China relations in view of Chinese involvement in strategic projects in Israel and focuses on the Bay Port project in Haifa. In conclusion, the article presents insights for Israel as a direct result of the Belt and Road Initiative, while examining the likelihood of diplomatic damage, security risks, and the effect on Israeli politicians as a result of this initiative.

Keywords: China, Sri Lanka, Israel, strategy, projects, Chinese initiative, Belt and Road Initiative

---

Shlomi Yass is an intern at INSS and a guest writer at the Forum for Regional Thinking.

1 Mark Melton, "China's Plan for a New World Order: Review of Maçães' Belt and Road," *Providence*, September 12, 2019, https://providencemag.com/2019/09/chinas-new-world-order-book-review-bruno-macaes-belt-road-initiative.

Introduction

A short time after being chosen as president of China in 2013, Xi Jinping announced what seemed to be the largest economic project in history—the "Belt and Road Initiative" (BRI). The initiative is the Chinese president's grand strategy to renew the ancient continental Silk Road by building a network of international fast train lines and roads that would join China with Africa and Europe, as well as by establishing a network of sea ports to create a maritime trading channel that would extend over a number of oceans.[2] As part of this strategy, China is also planning to expand existing aerial cargo agreements and to build a variety of facilities for energy, communications, manufacturing, and other needs.[3]

Significant progress in implementing this initiative was achieved in June 2015, when fifty-seven countries (excluding Japan and the United States) joined as founding members of a new bank in Beijing—"The Asian Infrastructure Investment Bank" (AIIB)—which had initial capital of $100 billion.[4] As of October 2019, China holds 31 percent of the bank's total capital, which gives it 26.6 percent of the voting rights; in other words, it can veto any decision that requires a special majority (of at least 75 percent of voters).[5] Israel also joined the AIIB as a founding country, assuming that this would help Israeli companies participate in the bank's projects.[6]

The first forum of the BRI convened in 2017. The United States took part in the conference, although with the lower-level participation by the

2 Mai Phan, "A Mixed Reality of The Belt and Road Initiative in Southeast Asia," *Journal of International Relations*, July 22, 2019, http://www.sirjournal.org/op-ed/2019/7/22/a-mixed-reality-of-the-belt-and-road-initiatives-in-southeast-asia.

3 Martin Hart-Landsberg, "A Critical Look at China's One Belt, One Road Initiative," *CADTM*, October 10, 2018, http://www.cadtm.org/A-critical-look-at-China-s-One-Belt-One-Road-initiative.

4 "Founding 57 Members of China-led AIIB Investment Bank Sign Up in Great Hall Ceremony," *Deutsche Welle*, June 29, 2015, https://www.dw.com/en/founding-57-members-of-china-led-aiib-investment-bank-sign-up-in-great-hall-ceremony/a-18546332.

5 Jason Kirk, "China and the Asian Infrastructure Investment Bank," *Observer Research Foundation*, November 1, 2019, https://www.orfonline.org/expert-speak/china-and-the-asian-infrastructure-investment-bank-55693.

6 Hagai Shagrir, *Israel-China Relations: Innovative Comprehensive Partnership*, Memorandum no. 194 (Tel Aviv: INSS, 2019), 21.

National Security Council's senior director of Asia Affairs.[7] In April 2019, the initiative's second forum took place, with thirty-six heads of state and government participating.[8]

The number of countries involved in the Chinese strategic initiative is impressive. As of March 2019, China had signed 173 cooperation agreements with 125 countries and twenty-nine international organizations. In addition, China had signed bilateral air traffic agreements with 126 countries and expanded existing air traffic agreements with various countries (including Israel). In the past five years, China has opened more than one thousand new international air routes.[9] In April 2019, Italy signed a memorandum of understandings with China as part of the BRI, and Russia recently joined the initiative as well, giving a green light to the construction of an international autostrada with China.[10] The World Bank estimates some $575 billion worth of energy plants, railways, roads, ports, and other projects have been built or are in the works as part of the Chinese initiative.[11]

In this context, it is worth mentioning other "silk roads" that China is currently building: The "Digital Silk Road," which is a network of undersea internet cables; the "Space Silk Road" (Beidou), which is a Chinese navigation system that is striving to replace the American GPS satellite network,[12] and the "Polar Silk Road," which aims to deal with shipping lanes, scientific research, climate change, and arctic resources.[13]

---

7 Matt Spetalnick and David Brunnstrom, "Trump Asia Expert to Become New Deputy National Security Adviser: Sources," *Reuters*, September 20, 2019, https://www.reuters.com/article/us-usa-trump-adviser/trump-asia-expert-to-become-new-deputy-national-security-adviser-sources-idUSKBN1W523F.

8 Shannon Tiezzi, "Who Is (and Who Isn't) Attending China's 2nd Belt and Road Forum?" *The Diplomat*, April 27, 2019, https://thediplomat.com/2019/04/who-is-and-who-isnt-attending-chinas-2nd-belt-and-road-forum.

9 "The Belt and Road Initiative Progress, Contributions and Prospects," *Belt and Road Portal*, April 22, 2019, https://eng.yidaiyilu.gov.cn/zchj/qwfb/86739.htm.

10 Alice Scarsi, "Russia and China Agree 5000-mile 'Moscow Bypass' Road to Strengthen Economic Ties," *Express*, July 10, 2019, https://www.express.co.uk/news/world/1151662/russia-news-china-Russia-Western-China-highway-Belt-and-Road-Initiative-bri.

11 "China's Belt and Road Gets a Reboot to Boost Its Image," *Bloomberg*, August 14, 2019, https://www.bloomberg.com/news/articles/2019-08-14/china-s-belt-and-road-is-getting-a-reboot-here-s-why-quicktake.

12 Matthew Johnson, "China's International Partnerships: Pakistan, CPEC and Central Asia," *Tibet Digest* (Foundation for Non-violent Alternatives) (August 2019), 98.

13 Qiyang Niu, "China's Evolving Arctic Policy: Two Geopolitical Threats," *Tibet Digest* (Foundation for Non-violent Alternatives) (August 2019), 116.

Challenges to the Belt and Road Initiative

The effects and the broad global implications of the Belt and Road Initiative also have drawn criticism and have exposed its shortcomings and weaknesses. China has promoted a narrative of "nonintervention," which states that any intervention in the politics or policy of the initiative's partner countries must be seen as if it was invited by their governments.[14] Basically, Chinese projects are only narrowly open to international participation. As of 2018, out of all contractors participating in Chinese-funded projects across the Eurasian supercontinent and tracked by Center for Strategic and International Studies, 89 percent belong to Chinese companies, 7.6 percent belong to local companies (companies whose head offices are located in the country in which the project is taking place), and 3.4 percent belong to foreign companies. Among the many projects included in the BRI are those that began years before the initiative was launched.[15]

In the past year-and-a-half (as of October 2019), the growth in the scope of the initiative slowed drastically. In 2018, the value of new projects in the sixty-one countries that are involved in the initiative had decreased by 13 percent compared with 2017; by August 2019, it had dropped another 6.7 percent. In the first eight months of 2019, existing contracts had further declined by 4.2 percent. A few countries participating in the initiative lowered planned loans and even cancelled projects, partly for economic or political reasons.[16] At least seven countries, including Pakistan, Myanmar, the Maldives, Kenya, and Sri Lanka, encountered problems with the initiative's projects or asked to reconsider them.[17] China's investment in other countries, especially within the framework of the BRI, raises issues concerning debt, threats to sovereignty, land grabbing, uprooting, human rights abuses in

14 Nicholas Crawford, *China and Instability in Developing Countries* (International Institute for Strategic Studies, October 28, 2019), 3, https://www.iiss.org/blogs/research-paper/2019/10/china-and-instability.

15 Jonathan E. Hillman, *China's Belt and Road Initiative: Five Years Later* (Center for Strategic and International Studies, January 25, 2018), https://www.csis.org/analysis/chinas-belt-and-road-initiative-five-years-later-0.

16 Cissy Zhou, "China Slimming Down Belt and Road Initiative as New Project Value Plunges in Last 18 Months, Report Shows," *South China Morning Post*, October 10, 2019, https://www.scmp.com/economy/global-economy/article/3032375/china-slimming-down-belt-and-road-initiative-new-project.

17 "China's Belt and Road Gets a Reboot to Boost its Image," *Bloomberg*, August 14, 2019, https://www.bloomberg.com/news/articles/2019-08-14/china-s-belt-and-road-is-getting-a-reboot-here-s-why-quicktake.

areas of dispute, environmental impacts, concerns over public health, and breaches of employment conditions.[18]

Several arguments have been raised against the initiative. The first argument views it as more than just an economic initiative and rather as a main tool for promoting Chinese geopolitical ambitions. Some believe that it is a Chinese reaction against the refocusing of the United States on Asia ("Pivot to Asia"), which began in 2011 during the Obama administration, and which many in Beijing view as an attempt to hinder China's influence by expanding US economic ties in southeast Asia. The United States and some of its allies have warned that the Chinese initiative may be really a "Trojan Horse" intended to promote Chinese regional hegemony and enable Chinese military and institutional expansionism.[19] A second argument views the Chinese initiative as a type of "debt-trap diplomacy" against developing countries. According to this argument, China is mortgaging the resources and strategic assets of developing countries in exchange for financing and building infrastructure in those countries, and it is working toward gaining preferential access to their natural resources. In this way, China achieves both economic penetration and strategic leverage.[20] A third argument views the initiative as causing environmental damage on a global scale. This is a legitimate concern due to the environmental impact of the initiative, particularly given the paucity of experience in analyzing the environmental impact of massive infrastructure development on the scale of the Chinese initiative.[21]

In June 2019, the World Bank published a study that attempted to answer these three arguments. The authors do not reject the Chinese initiative out of hand but recommend a series of profound changes, writing that "China's Belt and Road Initiative (BRI) could speed up economic development and reduce poverty for dozens of developing countries—but it must be accompanied by

18 GRAIN, *The Belt and Road Initiative: Chinese Agribusiness Going Global* (GRAIN, February 18, 2019), https://www.grain.org/en/article/6133-the-belt-and-road-initiative-chinese-agribusiness-going-global.

19 Andrew Chatzky and James McBride, "China's Massive Belt and Road Initiative," *Council on Foreign Relations*, May 21, 2019, https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative.

20 Ronak Gopaldas, "Lessons from Sri Lanka on China's 'Debt-Trap Diplomacy'" *Institute for Security Studies*, February 2, 2018, https://issafrica.org/amp/iss-today/lessons-from-sri-lanka-on-chinas-debt-trap-diplomacy.

21 Hoong Chen Teo and others, "Environmental Impacts of Infrastructure Development under the Belt and Road Initiative," *Environments* 6, no. 6 (2019): 1.

deep policy reforms that increase transparency, improve debt sustainability, and mitigate environmental, social, and corruption risks."[22]

China-Sri Lanka Relations Vis-à-vis Sri Lanka's Political System

The Chinese interest in Sri Lanka is, to a large extent, due to its strategic position, having served for many years as a large maritime trading junction in the Euro-Asian space. Sri Lanka can provide a convenient and rapid gateway to developing markets in the Indian subcontinent, meeting Chinese interests.[23] China's strategic closeness to Sri Lanka began with the administration of Sri Lankan president Mahinda Rajapaksa, who served between 2005 and 2015, during which China became Sri Lanka's main weapons supplier. While the United States halted direct military assistance to Sri Lanka in 2007, China increased its assistance to the island by about $1 billion and became the largest contributor to its economy and military. China provided sophisticated weapons to Sri Lanka, including six Chinese F-7 combat planes, and it encouraged Pakistan to sell weapons to Sri Lanka and train its pilots.

China also assisted Sri Lanka diplomatically and even cast a veto against the UN Security Council proposal to hold a discussion on Sri Lanka following the civil war on the island and perhaps to send UN observers there.[24] Economic relations between the two countries also strengthened to the point whereas in 2013, China became the greatest source of direct foreign investment in Sri Lanka.[25] President Rajapaksa relied increasingly on the Chinese in order

22 "Millions Could Be Lifted Out of Poverty, but Countries Face Significant Risks," *World Bank,* June 18, 2019, https://www.worldbank.org/en/news/press-release/2019/06/18/success-of-chinas-belt-road-initiative-depends-on-deep-policy-reforms-study-finds.

23 Marcello Rossi, "Next Hambantota? Welcome to the Chinese-funded US $1.4 billion Port City Colombo in Sri Lanka," *South China Morning Post*, May 12, 2019, https://www.scmp.com/week-asia/geopolitics/article/3009731/next-hambantota-welcome-chinese-funded-us14-billion-port-city.

24 "How Beijing Won Sri Lanka's Civil War," *The Independent*, May 23, 2010, https://www.independent.co.uk/news/world/asia/how-beijing-won-sri-lankas-civil-war-1980492.html.

25 N.P. Ravindra Deyshappriya, "China is Sri Lanka's Biggest Source of FDI, But There Is Room for More," *London School of Economics*, September 12, 2017, https://blogs.lse.ac.uk/southasia/2017/09/12/china-is-sri-lankas-biggest-source-of-fdi-but-there-is-room-for-more.

to build projects following the end of the civil war, and Sri Lanka borrowed more than $6 billion from China for that purpose.[26]

Chinese involvement in Sri Lanka became an important issue during the island's presidential election campaign in 2015. Mahinda Rajapaksa lost the election to Maithripala Sirisena, who promised to establish "equal relations" with India, China, Pakistan, and Japan, and to completely change the island's foreign relations. Sirisena wanted to distance himself from China—the ally of his predecessor Rajapaksa—and to draw closer to India and the West, while re-examining the Chinese projects.[27] Basically, his government was mainly concerned with reducing the damage done by previous governments.

Until 2015, about 95 percent of the Sri Lankan government's revenue was diverted to paying off the debt to China, which led it to conduct debt negotiations with China.[28] The debt to China in 2016 totaled $8 billion (close to 10 percent of Sri Lanka's GDP) and is mainly due to loans for building projects, most of which were approved during the Rajapaksa government.[29] The Sri Lankan government under Sirisena approved in that year to continue the projects, but they were subject to changes.[30] In 2017, it was reported that China had become the largest lender for building infrastructure projects in Sri Lanka (21.5 percent of total loans that Sri Lanka took out for building infrastructure projects), followed by Japan, the World Bank, and the Asian Development Bank (ADB).[31] In May 2019, President Sirisena met with

26 "Moving Away from China, Sri Lanka Puts Chinese 'Mega-Projects' on Hold," *AsiaNews/Agencies*, January 20, 2015, http://www.asianews.it/news-en/Moving-away-from-China,-Sri-Lanka-puts-Chinese-mega-projects-on-hold-33240.html.

27 Heather Timmons, "Sri Lanka's Election Upset just Destroyed a Linchpin of China's Foreign Policy," *Quartz Daily Brief*, January 9, 2015, https://qz.com/323718/how-sri-lankas-surprising-election-results-could-destroy-a-lynchpin-of-chinas-foreign-policy.

28 Jonathan E. Hillman, "Game of Loans: How China Bought Hambantota," *Center for Strategic and International Studies*, April 2, 2018, https://www.csis.org/analysis/game-loans-how-china-bought-hambantota.

29 Karthik Sivaram, "'Locked-In' to China: The Colombo Port City Project," *Freeman Spogli Institute for International Studies*, Stanford University, https://fsi.stanford.edu/publication/locked-china-colombo-port-city-project.

30 Shihar Aneez and Ranga Sirilal, "Sri Lanka to Allow Chinese Port City Project After Delay," *Reuters*, January 12, 2016, https://www.reuters.com/article/sri-lanka-china-portcity-idUSL3N14W42G20160112.

31 Nilanthi Samaranayake, "China's Engagement with Smaller South Asian Countries," *United States Institute of Peace*, April 2019.

Chinese president Xi Jinping and Chinese premier Li Keqiang during an international conference.[32]

In November 2019, an additional round of presidential elections was held in Sri Lanka. Outgoing president Sirisena did not stand for re-election, and Gotabaya Rajapaksa—the younger brother of former president Rajapaksa and who had served as defense minister in his brother's government from 2005 to 2015—was elected president. The spokesperson of the Chinese Foreign Ministry was quick to congratulate him, adding that "We are prepared . . . to work with the new government and leadership to cooperate at high levels surrounding the Chinese initiative, together with greater progress in bilateral relations, in order to bring about more tangible and other profits for both countries and their people."[33] Even during the election campaign, Gotabaya's associates announced that he planned to "restore relations" with Chinese president Xi Jinping.[34] Moreover, upon his election as president, Gotabaya Rajapaksa was quick to appoint his brother, former president Mahinda Rajapaksa, as the new prime minister and minister of finance.[35] These steps may indicate a new strategic closeness between Sri Lanka and China, even if it may develop more cautiously than in the past.

China-Sri Lanka: Four Main Projects

As stated, most of the Chinese loans in the Sri Lankan projects were given during the term of President Mahinda Rajapaksa. The four main projects in the country that were carried out with Chinese financing are the Hambantota Port; the international cricket stadium; the international airport at Hambantota; and the Port City of Colombo. All these projects are based on Chinese financing and were built by Chinese contractors. At least two of them have

32 "Li Keqiang Meets with President Maithripala Sirisena of Sri Lanka," *Ministry of Foreign Affairs of the People's Republic of China*, May 19, 2019, https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1664297.shtml.

33 "China Ready to Work with New Sri Lankan President," *Ada Derana*, November 18, 2019, http://www.adaderana.lk/news_intensedebate.php?nid=59134.

34 Shihar Aneez and Ranga Sirilal, "Record Number of Candidates to Contest Sri Lanka's Presidential Election," *Reuters*, October 7, 2019, https://www.reuters.com/article/us-sri-lanka-elections/record-number-of-candidates-to-contest-sri-lankas-presidential-election-idUSKBN1WM1FB.

35 "Sri Lanka President Pledges Election at 'Earliest Opportunity,'" *Al Jazeera*, November 22, 2019, https://www.aljazeera.com/news/2019/11/sri-lanka-president-pledges-election-earliest-opportunity-191122084348262.html.

long-term strategic implications for Sri Lanka (the Hambantota Port and the Port City of Colombo).

The Hambantota Port

The Hambantota Port is an example of Chinese "debt-trap diplomacy." The port, which sits along one of the most crowded strategic shipping lanes in the world, was built with a Chinese loan of about $1.3 billion—one of the largest initiatives built with Chinese government financing—and opened in 2010. However, despite that a large part of East-West trade passes through shipping lanes in the Indian Ocean, most ships bypass the Hambantota Port to anchor at the Colombo Port.[36] It quickly became clear that the new port was not profitable. Just thirty-four ships passed through it in 2012. Sri Lanka, which could not meet payments on the loan it received from China to build the port, asked for leniency in the terms of the loan but was turned down. In December 2017, the prolonged negotiations and the heavy financial pressure led the Sri Lankan government to accede to transfer the port to Chinese ownership and to agree to lease the sixty square kilometers of the project's land to China for ninety-nine years. The lease enabled China to take over territory that is just a few hundred kilometers away from its rival India, giving China a strategic foothold along a commercial and military sea lane of decisive importance.[37]

The international cricket stadium

In 2011, an international cricket stadium named after Mahinda Rajapaksa was opened near the town of Hambantota. It was built in order to host the Cricket World Cup, which took place that year in Sri Lanka. It is the second-largest stadium in Sri Lanka, holding 32,000 seats, and the cost of construction reached about $3.8 billion. Not long after it opened, criticism was leveled against it, firstly, the high cost of its maintenance, followed by the fact that since its construction, only a few international competitions have

36 Lu-Hai Liang, "Sri Lanka Hands Over Port to China to Pay Off Debt," *The National*, December 14, 2017, https://www.thenational.ae/world/asia/sri-lanka-hands-over-port-to-china-to-pay-off-debt-1.684606.

37 Maria Abi-Habib, "How China Got Sri Lanka to Cough Up a Port," *New York Times*, June 25, 2018, https://www.nytimes.com/2018/06/25/world/asia/china-sri-lanka-port.html.

been held there.[38] Since then, the stadium has become a "white elephant," housing birds and migratory animals, and reports say that it also hosts private events, including weddings.[39] It should be noted, however, that the international cricket stadium is not a Chinese geopolitical interest, compared to the Chinese investment in the Hambantota Port, which gives China clear geopolitical advantages.

The Hambantota International Airport

In 2013, the Mahinda Rajapaksa International Airport in the town of Hambantota opened to commercial air traffic. The cost of constructing the airport was $209 million, of which $190 million was borrowed from China. The congestion at the Bandaranaike International Airport in Colombo and the desire to narrow the gaps with other areas in Sri Lanka were the main motivating factors in building another international airport on the island. However, Hambantota lacks significant population and the industrial infrastructure needed to attract foreigners. It was not long before the new airport became known as "the world's emptiest international airport."[40] It also became clear that the airport was causing damage to the environment, since it is located in the heart of a nature reserve. In one instance it was reported that hundreds of soldiers, police officers, and volunteers were working to move the animals out of the airport area, and an official source even confirmed that the animals were interfering with flights. Moreover, during the first ever landing at the new airport, a plane's window was smashed when a bird hit it.

Like the cricket stadium, the Hambantota International Airport has become a "white elephant." At one stage, it was being used to store rice.[41] The situation changed in 2018, when India announced that it would operate the airport under a lease agreement for forty years and would invest $225

38 Nirmala Kannangara, "Hambantota White Projects Eat Up Economy," *Sunday Leader*, June 28, 2015, http://www.thesundayleader.lk/2015/06/28/hambantota-white-projects-eat-up-economy.

39 Hafsa Sabry, "Attempts To Revive Another 'White Elephant'" *Sunday Leader*, October 16, 2016, http://www.thesundayleader.lk/2016/10/16/attempts-to-revive-another-white-elephant.

40 Wade Shepard, "The Story Behind The World's Emptiest International Airport," *Forbes*, May 28, 2016, https://www.forbes.com/sites/wadeshepard/2016/05/28/the-story-behind-the-worlds-emptiest-international-airport-sri-lankas-mattala-rajapaksa/#3e385ee67cea.

41 "Troops Clear Wild Animals from Sri Lanka's White-Elephant Airport," *Phuket News*, March 27, 2016, https://www.thephuketnews.com/troops-clear-wild-animals-from-sri-lanka-white-elephant-airport-56780.php#fiXboQ2cffE7AXhv.97.

million to renovate it. The investment amounted to 70 percent of the cost of the renovation, with Sri Lanka covering the remaining amount.[42]

The Port City of Colombo

The foundations for the construction of the artificial port in Colombo were poured in 2014, and it was supposed to be built by pumping coastal sand from nearby beaches. The new port is expected to cover an area of 2.69 square kilometers alongside the Sri Lankan capital's main port.[43] The port represents the largest foreign direct investment in Sri Lankan history, which included a loan of $1.4 billion from the Chinese government-owned construction giant CCCC. The project is expected to include residential towers, luxury hotels, prestigious shopping malls, spacious parks, and 80,000 apartments, as well as providing daily employment for about a quarter million Sri Lankans once the project is completed.[44]

Since this is an additional strategic port being built under the Chinese initiative, there is a real concern that it too, like the Hambantota Port, will fall under Chinese influence. The statement by the Sri Lankan minister in charge of the project that the area from which the Chinese are pumping the sand will not threaten Sri Lanka's sovereignty and will not undermine India's interests,[45] did not calm the situation, particularly since Chinese warships and submarines have been anchored at the Colombo Port as early as 2014, despite Indian objections. Moreover, hundreds of warships from various countries anchor at the Colombo Port for refueling and refreshing. But the frequency of Chinese visits and the fact that Chinese submarines anchored at a port on the Indian Ocean as part of a Chinese military operation against pirates in

42 Meera Srinivasan, "'Mattala Project with India Is on,'" *The Hindu*, August 3, 2018, https://www.thehindu.com/news/international/mattala-project-with-india-is-on/article24595483.ece.

43 "Feature: Hearts Bound Together, City Built Together—China, Sri Lanka Co-Develop Colombo Port City," *Xinhua*, May 15, 2018, http://www.portcitycolombo.lk/press/2018/05/23/hearts-bound-together-city-built-together-China-sri-lanka-co-develop-colombo-port-city.html.

44 Rossi, "Next Hambantota? Welcome to the Chinese-Funded US$1.4 billion Port City."

45 "Chinese Firm Completes US$1.4 Billion Land Reclamation Works for Sri Lanka's Colombo Port City Project," *South China Morning Post*, January 17, 2019, https://www.scmp.com/news/asia/south-asia/article/2182461/chinese-firm-completes-14-billion-land-reclamation-works-sri.

the Gulf of Aden are not routine occurrences.[46] If that is not sufficient, the construction of the Port City of Colombo has brought with it environmental damage. The pumping of sand in order to build the artificial port has caused erosion and has interfered with the maritime ecological system, which, in turn, have damaged the fishing industry in the area.[47]

Israel-China Relations: Economic Interests

Although Israel was the first country in the Middle East to recognize the People's Republic of China in January 1950, diplomatic relations between the two countries were only established in January 1992. Since then, cooperation has developed in a variety of areas, reaching new peaks in recent years. Israeli representatives in China are promoting Israel's image as a technologically innovative country, and the two countries are engaging in joint projects in research, scientific, academic, agricultural, and healthcare innovation.[48]

In 2014, the main intergovernmental mechanism between Israel and China—the innovation conference—was established. This is an intergovernmental (G2G) platform established by Israel's Prime Minister Benjamin Netanyahu and China's Vice-Premier Liu Yandong during her visit to Israel that year. The conference convenes every other year alternating between Beijing and Jerusalem and is led by thirteen government ministries and agencies in Israel, alongside ministers from the Chinese government. The conference promotes cooperative ventures between governments in both countries, joint projects involving the private sector, joint scientific and industrial research, provides grants for students from both countries, and more.[49]

---

46 Shihar Aneez and Ranga Sirilal, "Chinese Submarine Docks in Sri Lanka Despite Indian Concerns," *Reuters*, November 2, 2014, https://www.reuters.com/article/sri-lanka-china-submarine/chinese-submarine-docks-in-sri-lanka-despite-indian-concerns-idINKBN0IM0LU20141102.

47 Rossi, "Next Hambantota? Welcome to the Chinese-Funded US$1.4 billion Port City."

48 "25 Years of Diplomatic Relations between Israel and China," *Ministry of Foreign Affairs*, January 23, 2017, https://mfa.gov.il/MFAHEB/PressRoom/Spokesman/2017/Pages/25-years-Israel-China-diplomatic-relations-230117.aspx [Hebrew].

49 "Visit by the Chinese Vice-President—The Fourth Meeting of the Israel-China Innovation Committee," *Ministry of Foreign Affairs,* October 18, 2018. https://mfa.gov.il/MFAHEB/PressRoom/Spokesman/2018/Pages/Visit_of_Vice_President_of_China_181018.aspx [Hebrew].

China has bought Israeli companies, such as Tnuva, Adama, and Ahava, and has invested in Israeli startups and venture capital funds.[50] In addition, China was involved in construction of the Carmel Tunnels, the Akko-Karmiel train line, the Tel Aviv Light Rail, the privatization of the Ashdod and Haifa ports, the Tel Aviv-Jerusalem train line, and the planned train line between Tel Aviv and Eilat.[51]

Relations between Israel and China were furthered when Prime Minister Netanyahu visited China in 2017, as well as by Chinese president Xi Jinping's rebranding of cooperation between the two countries as an "Innovative Comprehensive Partnership."[52] The upgrading in relations was partly the result of the strengthening of the connection and dialogue between government entities as well as due to interests such as the desire to gain access to Israeli civilian technologies and the Israeli drive to access the Chinese market. This is in addition to strengthening academic and research contacts and encouraging the movement of people from both countries.[53]

The trade ties that Israel currently has with China are among the largest and most important for Israel out of all other countries. In the past decade, the two countries have experienced a sharp increase in the volume of trade (although in an inequal manner). China is the largest source of imports to Israel, and the third largest destination for exports (if the European Union is considered a single entity). This is reflected in an increase in both exports and imports. In 2018, the volume of trade between Israel and China was about $15.7 billion (an increase of about 30 percent compared with 2017). In 2018, exports to China totaled $4.7 billion (a jump of about 50 percent compared with 2017), while imports from China totaled about $11 billion (an increase of about 20 percent compared with 2017). The dominance of

50 Dan Catarivas, "Israel-China Relations: Ideal and Reality" in *Israel-China Relations: Opportunities and Challenges*, ed. Assaf Orion and Galia Lavi, Memorandum no. 194 (Tel Aviv: INSS, 2019), 30.

51 Yossi Melman, "Cause for Concern? Chinese Investment and Israel's National Security," *Jerusalem Post*, April 7, 2018, https://www.jpost.com/Jerusalem-Report/Chinese-TAKEAWAY-546692.

52 "Strengthening Israel-China Cooperation in Innovation and Technology," Ministry of Economy and Industry, August 19, 2018. https://www.gov.il/he/departments/news/a-billion-chinese-are-not-mistaken [Hebrew].

53 Shagrir, *Israel-China Relations: Innovative Comprehensive Partnership*, 14.

imports from China in the balance of trade between the two countries means that Israel has a continuing trade deficit with China.[54]

Haifa Port

In 2004, Israel began the process of privatizing its three commercial ports—Ashdod, Eilat, and Haifa. At the end of the process, the Israel Ports Authority had been replaced by four government companies, with the aim of separating the ports' management and future development from their day-to-day operations. It was decided that the Israel Ports Company would provide the infrastructure and be responsible for its development, while the private companies would provide cargo shipping services, using their own facilities and equipment.[55]

In 2014, the SIPG company (a subsidiary of "China Harbor," itself a subsidiary of CCCC, which, as stated, is owned by the Chinese government) won the tender to build a new port in Ashdod over a seven-year duration at a cost of NIS 3.6 billion. In 2015, the SIPG Group also won a tender to operate the future port in Haifa for twenty-five years, in exchange for on-going usage fees that it would pay to the State of Israel. The cost of building the port was estimated at $2 billion, and it is expected to begin operating in 2021.[56] The Israel Ports Company says that the international operators will plan, finance, and build the operational areas, including completion of various infrastructure systems.[57]

The new port in Haifa is an example of Chinese strategic-security involvement in Israeli infrastructure. This is one of the crown jewels in the pro-Chinese trend being led by Yisrael Katz, the former minister of transportation and road safety. As part of this trend, a Chinese news crew came to Israel in May 2017, and Minister Katz gave them a personal interview. The Chinese media also published a story that Katz took an active role, ever since

54 "Israel-China: A Review of Economic Trade," Israel Export Institute—Economic Unit, 2018. https://www.export.gov.il/economicreviews/article/israelchinacom2018 [Hebrew].

55 Oded Eran, "China Has Laid Anchor in Israel's Ports," *Strategic Assessment* 19, no. 1 (April 2016): 56.

56 "Haifa Container Terminal Deal with China's SIPG Under Review," *PortSEurope*, December 23, 2018, https://www.portseurope.com/haifa-container-terminal-deal-with-chinas-sipg-under-review.

57 Lior Gutman, "The Chinese SIPG Company Won the Tender to Operate the New Port in Haifa," *Calcalist*, April 23, 2015. https://www.calcalist.co.il/local/articles/0,7340,L-3655245,00.html [Hebrew].

being appointed to the position, in infrastructure projects between the two countries, and that he was given more exposure due to Chinese involvement in the construction of the new port at Ashdod and the operation of the new port in Haifa Bay. As reported, Minister Katz referred to this involvement as "a strategically important step for Chinese companies."[58]

In June 2019, the Municipality of Haifa filed an administrative appeal with the Haifa District Court to prevent continued construction of the new port in the city, arguing that the municipal airport would be harmed and that construction of the port would prevent the extension of its runway. Haifa's mayor, Einat Kalisch-Rotem, complained that no in-depth research had been done to understand the ramifications of the unilateral moves on the advancement of shipping and aviation in the city.[59] In August 2019, Kalisch-Rotem tweeted that she had reached agreements with the Ministry of Transportation to extend the runway at the Haifa airport to 2,100 meters, withdraw the appeals against the Haifa Port, and fix the coastal erosion.[60]

The new Haifa Port, with its military and civilian infrastructure, is a strategic asset for Israel. Therefore, Chinese involvement in its construction and operation could in the future affect the continuous traffic of goods to and from the port and serve as a tool of influence on Israel.[61] However, when examining Chinese involvement in the Haifa Port versus the Hambantota Port in Sri Lanka, significant difference between the two cases can be discerned. In the case of Israel, the expansion and operation of the Haifa Port is not dependent on a Chinese loan, while in the case of Sri Lanka, the construction of the Hambantota Port was based on a large Chinese loan with all that that entailed.

58 Dubi Ben-Gedalyahu, "Israeli Minister's Chinese Romance Provokes US," *Globes*, December 20, 2018, https://en.globes.co.il/en/article-israeli-ministers-chinese-romance-provokes-us-1001265841.

59 Michal Raz-Haimovitch and Daniel Shmil, "The Municipality of Haifa Opposes Continued Construction of the Port: 'It Will Destroy Aviation in the City,'" *Globes*, June 16, 2019. https://www.globes.co.il/news/article.aspx?did=1001289748 [Hebrew].

60 Einat Kalisch-Rotem, Twitter, August 14, 2019. https://twitter.com/EINATkalisch/status/1161648831894872064?ref_src=twsrc%5Etfw [Hebrew].

61 Galia Lavi and Rotem Nusem, "The Rising Tension between China and Australia: Lessons for Israel," in *Israel-China Relations: Opportunities and Challenges*, ed. Assaf Orion and Galia Lavi, Memorandum no. 194 (Tel Aviv: INSS, 2019), 36–37.

Risks and Conclusion

Senior officials in the Israeli government estimate that Israel is the only country in which Chinese companies have invested in or gained access to projects worth about $15 billion.[62] One of the reasons is Israeli regulation, which is decentralized in terms of foreign investment and purchases in civilian areas, with each government entity or ministry independently operating its own regulator.[63] Member of Knesset Ofer Shelah said in this regard that an "inclusive policy" was necessary, particularly regarding China; otherwise, each government ministry would "determine policy on its own."[64] The former head of Israel's National Security Council, Jacob Nagel, proposed establishing an inter-ministerial regulatory committee with the participation of all involved parties, which would "have authority, and not just [be] something to provide recommendations."[65]

Israel's cabinet recently decided to establish an advisory committee led by the Ministry of Finance to examine national security aspects of the process to approve foreign investments in Israel, as is customary in countries such as the United States, Canada, the United Kingdom, Germany, Australia, and others.[66] However, as opposed to committees working in those countries, the committee in Israel will be established on a voluntary basis and not as part of legislation dealing with foreign investments. It will consult with regulators, but not with senior political officials, and reporting to it will be voluntary and not obligatory. In addition, various technologies, which are a hot topic between the United States and Israel, will not require the committee's supervision.[67]

---

62 Yossi Melman, "Over U.S. Objections, Chinese Firms Step Up Their Involvement in Israel," *Jerusalem Post*, July 13, 2019, https://www.jpost.com/Jerusalem-Report/Over-US-objections-Chinese-firms-step-up-their-involvement-in-Israel-595325.

63 Doron Ella, "Regulation of Foreign Investments and Acquisitions: China as a Case Study," in *Israel-China Relations: Opportunities and Challenges*, ed. Assaf Orion and Galia Lavi, Memorandum no. 194 (Tel Aviv: INSS, 2019), 61.

64 Melman, "Cause for Concern? Chinese Investment and Israel's National Security."

65 Jacob Nagel, "Ex-National Security Advisor to 'Post': Israel Needs to Review China Deals," *Jerusalem Post*, January 10, 2019, https://www.jpost.com/Opinion/Ex-national-security-advisor-to-Post-Israel-needs-to-review-China-deals-576891.

66 "Announcement by the Ministerial Committee on National Security," Prime Minister's Office, October 30, 2019. https://www.gov.il/he/departments/news/spoke_national_security301019.

67 Doron Ella, "A Regulatory Mechanism to Oversee Foreign Investment in Israel: Security Ramifications," *INSS Insight* no. 1229, November 19, 2019, https://www.inss.org.il/publication/a-regulatory-mechanism-to-oversee-foreign-investment-in-israel-security-ramifications.

These disadvantages may be an opening for diplomatic damage, security risks, and influence on Israeli politicians.

Potential diplomatic damage as a result of Chinese involvement in strategic projects in Israel may also result from conflicts of interests between the United States and China, with Israel caught in the middle. The potential for harm to Israel's close relations with the United States due to Chinese involvement in Israel is reflected in a study by the Center for a New American Security (CNAS), which states that construction of the Haifa Port may pose geopolitical risks. In addition, John Bolton, former US national security advisor, expressed concern over future Chinese control of operations at Israeli ports, particularly emphasizing the fact that the Haifa Port hosts military maneuvers between Israel and the United States on a regular basis and also serves as an anchorage for the American Sixth Fleet, which operates in the Mediterranean.[68] In addition, US Deputy Energy Secretary Dan Brouillette sounded explicit warnings, saying that "if Israel deepens this cooperation, we may not share intelligence information with it."[69]

Most of the security risks from close cooperation with China are due to Chinese investment in strategic Israeli infrastructure and Chinese penetration of that infrastructure and of various Israeli technology companies. In this context, Head of the Israel Security Agency Nadav Argaman warned that "Israeli law lags behind security needs in terms of supervision of investments by foreign countries," and even warned that "Chinese influence in Israel is dangerous, particularly in regard to strategic infrastructure and large corporations."[70] Former head of the Mossad Efraim Halevy also spoke in this regard, saying that despite the fact that he does not oppose commercial relations with China, he is opposed "to any action that would lead to Chinese control over a main strategic transport artery in Israel." Halevy also warned

68 Daniel Kliman, Rush Doshi, Kristine Lee, and Zack Cooper, *Grading China's Belt and Road*, (Center for a New American Security, April 8, 2019), 14, https://www.cnas.org/publications/reports/beltandroad.

69 Army Radio, Twitter, January 15, 2019. https://twitter.com/glzradio/status/1085404578122776576.

70 "Shin Bet Chief Said to Warn Chinese Investment in Israel Poses Security Threat," *Times of Israel*, January 10, 2019, https://www.timesofisrael.com/shin-bet-chief-said-to-warn-chinese-investment-in-israel-poses-security-threat.

that if China takes over the Ashdod-Eilat train line, it will gain control over a "point of political and economic control" within Israel.[71]

In addition to those who have reservations, others believe that the main risk of increasing Chinese investments in Israel is not due to the implications of investment in strategic infrastructure but from investment in Israeli technology companies. According to this argument, investment in such companies may allow China to develop technologies in the future that are based in Israel, damaging Israel's relations with the United States and impairing Israel's international economic competitiveness.[72]

Another risk due to increasing investment is the potential influence on politicians. Such influence may take place, for instance, as a result of unregulated Chinese (or other) involvement. Even though the Parties Financing Law from 1973 and the Parties Law from 1992 prohibit Israeli parties from receiving contributions from entities that do not have the right to vote for the Knesset, there is nothing to prevent such contributions from being made directly to politicians.[73]

In this regard, a CNAS study determined that China has bribed politicians and bureaucrats in the kleptocratic countries where it has invested its projects.[74] For instance, in 2016, the Sri Lankan minister of finance accused the Rajapaksa government of inflating the true cost of building the stadium in Hambantota and publishing a cost at the time that was four times the actual cost.[75] This was despite the stadium not having any strategic value to China. It was also reported that Chinese companies bribed the family of former Sri Lankan president Rajapaksa. Agreements were also reportedly signed in Malaysia with Chinese companies for inflated values, and some of the money was reportedly passed on to politicians. Bangladesh blacklisted

71 "Former Mossad Chief Efraim Halevy Warns Against China's Role in Israeli Rail," *Economic Times*, October 5, 2013, https://economictimes.indiatimes.com/former-mossad-chief-efraim-halevy-warns-against-chinas-role-in-israeli-rail/articleshow/23579256.cms.

72 Yoram Evron, "Chinese Investments in Israel: Opportunity or National Threat?," *INSS Insight* no. 538, April 8, 2014, https://www.inss.org.il/publication/chinese-investments-in-israel-opportunity-or-national-threat.

73 Lavi and Nusem, "The Rising Tension between China and Australia: Lessons for Israel," 39.

74 Kliman, Doshi, Lee, and Cooper, *Grading China's Belt and Road*, 6.

75 "Ravi K Says Actual Cost of Hambantota Cricket Stadium Is Rs. 852 Million, And Not Rs. 4.5 Billion As Claimed By Rajapaksa," *Colombo Telegraph*, July 23, 2016, https://www.colombotelegraph.com/index.php/ravi-k-says-actual-cost-of-hambantota-cricket-stadium-is-rs-852-million-and-not-rs-4-5-billion-as-claimed-by-rajapaksa.

the China Harbor company due to attempted bribery of a senior government politician. It was also reported that Chinese companies paid the son of the president of Equatorial Guinea and its vice president millions of dollars. Pakistan stopped projects of the Chinese Belt and Road Initiative out of concern for corruption, and the former vice president of Ecuador was under investigation due to reportedly having received bribes from China.

The Chinese willingness to pay politicians to make it easier to carry out projects and the latter's readiness to receive bribes harm democratic institutions and conflict with the public interest.[76] It arouses suspicion, particularly when the terms of transactions of these projects being carried out as part of the Chinese initiative are immersed in secrecy, which arouses concern that local politicians will profit from them more than their citizens do.[77]

This situation may take place not only in kleptocratic democracies. It turns out that politicians in Australia also received contributions from Chinese businesspeople in exchange for support of Chinese policy.[78] Under the foregoing circumstances, we should not discount the possibility of future Chinese (and other) influence on Israeli politicians and bureaucrats who are involved in setting policy and decision making in the State of Israel.

76 Kliman, Doshi, Lee, and Cooper, *Grading China's Belt and Road*, 6–7.

77 "China's Belt-And-Road Plans Are to Be Welcomed—and Worried About," *Economist*, July 26, 2018, https://www.economist.com/leaders/2018/07/26/chinas-belt-and-road-plans-are-to-be-welcomed-and-worried-about.

78 A. Odysseus Patrick, "This Chinese Mogul Made Powerful Friends in Australia. Now He's a Case Study on Worries over Beijing's Influence," *Washington Post*, October 7, 2019, https://www.washingtonpost.com/world/asia_pacific/this-chinese-mogul-made-powerful-friends-in-australia-now-hes-a-case-study-on-worries-over-beijings-influence/2019/10/05/c5f7f1e6-dea9-11e9-be7f-4cc85017c36f_story.html.

Criminal Law as a Tool for Dealing with Online Violence among Youth

Limor Ezioni

This article seeks to examine whether criminal law is equipped to deal with the phenomenon of online violence among youth. In many cases, criminal law is not the optimal way to deal with online violence; therefore, it should only be used as a last resort, while being particularly cautious, especially when violence is not the result of a "criminal" nature but rather is the nature of the internet, which leads normative minors to carry out prohibited acts. The preferred means is to deal a-priori with the phenomenon, namely, to focus on education and prevention rather than punishment after the fact. This is a social issue with utmost importance, which parents, children, and educators should be aware of.

Keywords: Bullying, online violence, youth, minors, cyber, criminal law, education, prevention

Introduction

Protection of children and teens from online violence should be carried out on several levels, first and foremost, at the educational level, with activities directed at teachers, children, and parents. New methods and means of dealing with this phenomenon need to be developed, and the entire framework around the youth—family, friends, and educational staff—should be involved in creating and implementing programs to address online violence. The case of online violence enables and invites a particularly close cooperation between educational staff and parents.

Adv. Dr. Limor Ezioni is a senior lecturer at the Academic Center for Law and Science and a senior researcher at the Cyber Security Program at the INSS. For more on the topic of this article, see her book *Youth in Law* (Nevo Publishers, 2019) [Hebrew].

It is important that both educational staff and parents get to know and understand the online environment and its inherent dangers. It should also be remembered that violence that begins in school often continues online while bullying and violence in the virtual sphere often spill into the physical school environment. School staff are therefore required to be vigilant beyond school hours. Furthermore, conversations should be held with children in order to raise awareness to this phenomenon, to make them understand the consequences of their actions, and to encourage them to seek help if and when it is needed.

Online violence also needs to be tackled at the level of public regulation. Regulation should establish the rules of the game and the means of protecting minors who stand to be harmed by violating those rules. In addition, voluntary self-regulation on websites and social networks is needed.

Over the past decade, internet use has expanded to such a degree that it has become an indispensable part of our lives on many levels: on the professional level, in our conduct as consumers, in our contact with the authorities, as our source of knowledge, and also as a social space for managing relationships. Using social networks has become most popular among youth in Israel and around the world. Research in the United States and Europe shows that 60–65 percent of children ages nine and over use social networks and that rate rises to over 80 percent among teenagers. A study conducted in Israel by Bezeq Telecommunications in 2018 showed that 95 percent of Israeli teenagers between the ages of thirteen and eighteen use WhatsApp; 88 percent are active on Instagram; and 65 percent are active on Facebook. In addition, 43 percent of parents did not restrict their children's social media use during that year, whereas in the previous year, 2017, 50 percent of parents limited social media use to two hours a day.[1]

The internet, and especially social networks, has become an integral part of the day for most teenagers and even for younger children. The use of social networks by minors has many advantages: learning and expanding horizons, exposure to new content and new worlds, creativity and self-expression, and even for building social connections and developing a sense of belonging. However, the internet can also expose minors to dangers: It can be a source of negative influence, dangerous behavior, overstepping of boundaries, and

1 "Report on the Digital Life 2018," Bezek Telecommunications, https://www.bezeq.co.il/media/PDF/doh_2018.pdf [Hebrew].

exposure to abusive and harmful content. The internet's negative influence on minors is a very broad topic and can be discussed in many contexts, from the exposure of minors to pornographic content to online solicitation of minors by sex offenders seeking to exploit them. This article will address only one negative aspect of the exposure of minors on the internet, namely, that of online violence among minors.

Violent conduct on the internet presents a host of challenges, among them educational, social, and legal that the criminal law is required to address. Below, we will explore the phenomenon of online violence, focusing on those cases where both parties—the assailant and the victim—are minors. The discussion will revolve around the question of whether the Israeli criminal law is equipped to deal with this phenomenon.[2]

Definition

"Online violence," also known as "cyberbullying,"[3] can be defined as the use of information and technology by an individual or a group in order to hurt others through repeated, intentional, and aggressive behavior. Online violence is a new category of violence, inflicted through a variety of electronic devices, such as smartphones and computers, and expressed mainly on social networks, such as WhatsApp, Facebook, Instagram, and Snapchat. Online violence follows a person everywhere—in the minor's home, at school, at a party, or while out with friends. It may include harassment; gossip; messages of an insulting, degrading, and even threatening nature; impersonation; public distribution of material related to personal privacy; extortion; and use of webcams to transfer abusive content, such as photos and videos. The person inflicting the online violence may know the target person in "reallife" or might only know the target in the "virtual" online sphere.

The definition of online violence as "intentional and aggressive with the aim of harming others" creates difficulties, especially when the discussion concerns minors. Elsewhere, I have stated that "while we are mostly talking

2 In a different article, I extensively addressed the issue of violence on the online playground, emphasizing the responsibility of content providers and site operators for incidents on their turf. See Limor Ezioni, "Bullying on the Online Playground—Responsibility of Content Providers and Website Operators for Incidents on their Turf," *HaMishpat* 16 (2013): 463–513 [Hebrew].

3 I prefer to employ the term "online violence" rather than "cyber bullying," since the term "bullying" has a connotation of horseplay committed by minors as part of their youthful exuberance, while the acts I will discuss here are in no way trivial.

about the use of words and images, the boundary between simple harassment, which unfortunately is a characteristic of relationships in general and among children in particular, and between 'intentional and aggressive behavior aimed at causing harm' is unclear. Furthermore, behavior can also be ignoring or ostracizing from a particular social space. Phenomena such as boycotting [a person] or preventing [them] from participation are extremely powerful."[4] The difficulty in defining the phenomenon also creates problems with properly handling it, yet it should not be inferred from this difficulty that criminal law is unable to deal with the cases that constitute an offense.[5]

Ways of Expressing Online Violence Among Minors

The range of violent behaviors is endless, limited only by the imagination. The most common and simple behavior is sending a large number of emails, text messages, through posts on social networks such as Facebook or WhatsApp to a person who is not interested receiving them.[6] The content may include threats to cause harm, sexual references, hate speech, and so forth. The type of online violent behavior among minors can be categorized as follows:

4 Ezioni, "Bullying on the Online Playground," 470.

5 Moreover, in many rulings in recent years, it seems increasingly understood that as the virtual environment has become an indispensable part of social life, crimes committed within this environment must be recognized and severely punished. For example, Justice Daphne Barak-Erez remarked that "when considering the new ways of connecting people, using the various means made available to us by modern technology, an obscene act can be committed through the use of emails, images on a computer, and more. In a world in which it is possible to maintain a connection between people through the use of wires, frequencies, and electronic messages, an obscene act can be committed against a 'person' through those very means." See 7225/11 *John Doe v. State of Israel* (published in Nevo, January 24, 2013).

6 An example of an extreme case is that of David-El Mizrahi, who committed suicide after being abused on Facebook. The abuse included obscenities, humiliation, and harassment. Another example is that of Rebecca Ann Sedwick, an American girl who committed suicide after receiving hate messages on social networks from two girls who goaded her into committing suicide. For further cases, see Anat Lior, "Cyber Bullying—A Wake-up Call for the Israeli Legislator," Law and Business Website, https://idclawreview.org/2013/11/17/blogpost-20131117-lior/.

- *Harassment*—repeatedly sending numerous and abusive messages (profanities, insults, threats) to the victim through instant messaging, mobile phone messages, or through posts or messages on social networks.[7]
- *Raging*—abusive, crude, and insulting exchanges in discussions on forums, in chat rooms, and in WhatsApp groups. Those involved are usually drawn into aggressive behavior and the atmosphere becomes combative and offensive.[8]
- *Defamation*—disseminating mendacious stories and false information about a person to many acquaintances. The aim of defamation is to destroy the reputation of the victim as well as the victim's connections and social standing.
- *Masquerading*—using the victim's personal details in order to impersonate the victim and carry out actions under the victim's name. For example, a boy goes online under another boy's name and sends an abusive email to several friends.[9]
- *Outing and Deception*—exposing intimate and private information about a minor. For example, exposing an anonymous blog and identifying it with a specific person (a phenomena typical to content connected to sexual tendencies), or disseminating personal photos and videos on the internet.[10]

---

7 According to criminal appeal 9152/06 *John Doe v. State of Israel* (published in Nevo, February 19, 2007), which describes a case in which minors harassed another minor, inter alia, through threatening voicemail messages and via the computer; and according to appeal of criminal sentencing 259892-01-11 *Huri v. State of Israel* (published in Nevo, February 9, 2011), in which the appellant and the complainant met on an online dating site and after several dates, the complainant sought to terminate the relationship. As a result, the appellant began to harass her by calling her numerous times and cursing her.

8 It is noteworthy that computer combat games often allow harassment of a minor's virtual character, such as by ganging up against the character or attacking the character which deviates from the official goal of the game.

9 According to criminal motions 4820/15 *State of Israel v. John Doe* (published in Nevo, July 14, 2015), in which the appellant broke into the Facebook account of a minor in order to liaison with female minors.

10 Criminal appeal 2656/13 *John Doe v. State of Israel* (published in Nevo, January 21, 2014), where it is stated that the appellant photographed minors without their knowledge during correspondence between them and threatened to publish the photos if they did not do as he asked. For more on the dissemination of photographs among children and teenagers on the internet, see Eti Weissblai, "Dissemination of abusive photos on the internet by children and teens," Knesset, Research and Information Center, 2010 [Hebrew]. See also criminal appeal 6357/11 *Braverman v. State of Israel* (published in Nevo, December 26, 2013), where the appellant was convicted for several sex offenses against minor teenaged girls, whom he met on social networks and seduced.

- *Exclusion*—internet boycott, in which an entire group ostracizes a minor from social arenas. For example, an entire class boycotts a child or does not accept the child's Facebook friendship requests.
- *Stalking*—tracking a minor in order to obtain details and personal information for the purpose of hurting, blackmailing, or terrorizing the person.
- *Threatening* —of all different types within a personal content, such as threats of self harm or to the life of another person. Online threats can be made via instant messaging programs, email, social networks, and more.[11]

Special Characteristics of Online Violence

"The computer screen, which is the tool that visually displays the electrical signals received from the computer, largely reflects the bipolar character of the internet. The transparent glass at the front of the screen opens before us a window to broad and rich information and to new worlds. The back part of the screen, on the other hand, is opaque and sealed and can resemble the darkness in which we find ourselves in relation to the true identity of the people on the other side of the network."[12]

The use of the internet has its own unique traits, as does the violence committed on it.[13] Anonymity enables a minor to share with others or to reveal personal details about another without being exposed. Most victims of online violence are not familiar with their assailant, who is able to maintain a false identity and remain anonymous.[14] Absolute anonymity releases inhibitions, and it even awakens evil in some people. Moreover, absolute anonymity can lead to exaggerated expression of negative feelings, not taking into account the norms and limitations of the "real world."[15]

---

11 Criminal appeal 538/13 *Sabah v. State of Israel* (published in Nevo, December 26, 2013), in which the appellant threatened several minors that if they did not fulfil his demands he would harm himself and tell their families about their sexual deeds with him. He even threatened to commit suicide.

12 Justice Hendel in criminal appeal 2656/13 *John Doe v. State of Israel* (published in Nevo, January 21, 2014).

13 Idit Avni and Avraham Rotem "Cyberbullying," *IAN Ethics,* 3 (2009) [Hebrew], ianethics.com/wp-content/uploads/2009/10/cyberBullying_IA_oct_09.pdf.

14 Wannes Heirman and Michel Walrave, "Assessing Concerns and Issues on the Mediation of Technology in Cyberbullying," *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 2, no. 2 (2008), https://cyberpsychology.eu/article/view/4214/3256.

15 "Many studies conducted in the United States and the European Union indicate that there is a high chance that youth with a social network profile events will be involved in incidences of online abuse. Studies show that the highest rate of online abuse, some 41%, is among girls aged 15–17." See Lior, "Cyber Bullying—A Wakeup Call for the Israeli Legislator."

Furthermore, in the real world, violence and harassment occur in a circumscribed domain—within school boundaries, among friends, in after-school activities—while the internet allows for a wide and rapid circulation to a large number of users. Thus, youth can use the internet to mock and insult other youths. For example, in one case, a minor girl was abused by another girl on various social networks. Among other things, the assailant disseminated pornographic videos with the girl's head superimposed in a Facebook group of some 90,000 youths, resulting in profanities, threats, and abuse from youth who did not even know the victim.[16] Those involved in online violence have the ability to circulate messages, photos, or any other material to a large and diverse audience, and the assailant is often unaware of the snowballing effect that he has caused.[17]

The phenomenon of online violence is also unique because of the accessibility of the internet anywhere and any time, thus completely blurring the boundary between the whereabouts of the abuser and the victim. In the past the victim had refuge from harassment in thier home, today, internet harassment leaves the victim with nowhere to escape, as the harassment penetrates into the private space.[18]

Dealing with the Phenomenon on the Level of Criminal Law

Despite existing restrictions on the use of criminal law in dealing with online violence, the criminal law may be the appropriate arena for dealing with some cases. In general, these cases can be divided into two types: The first includes cases where it is obvious that if the violence occurred in the real world rather than the online world, it undoubtedly would constitute a criminal offense. A striking and clear example is photographing a minor in an intimate situation without the minor's knowledge and consent and subsequently circulating the photograph via the internet. The second type

16 For more on this subject, see Liron Shamam, "The Writing on the Wall," *Mako*, April 11, 2013 [Hebrew], www.mako.co.il/nexter-weekend/Article-6554514438eed31006.htm.

17 Michele L. Ybarra and Kimberly J. Mitchell, "Online Aggressor / Targets, Aggressor and Targets: A Comparison of Youth Characteristics," *Journal of Child Psychology and Psychiatry* 45, no. 7 (2004):1308–1316.

18 Janis Wolak, Kimberly J. Mitchell, and David Finkelhor, "Does Online Harassment Constitute Bullying? An Exploration of Online Harassment by Known Peers and Online-Only Contacts," *Journal of Adolescent Health*, 41, no. 6 Supplement (December 2007): S51–S58.

involves violent acts between minors that are unique to the virtual world but the consequences (or potential consequences) thereof are particularly grave and thus require a penal response.

In Israel, there is no specific legislation prohibiting online violence (cyberbullying), and this applies all the more so to criminal legislation. In the absence of a special provision, acts performed in the virtual environment must be examined in the criminal context—whether the elements of *actus reus* and *mens rea* have been fulfilled. Nonetheless, Israel does have legislation that deals with criminal prosecution of a minor who had circulated videos of a sexual nature. In 2014, a new article was added to the Prevention of Sexual Harassment Law,[19] dubbed by the media as "the Videos Law." The article states that sexual harassment will also include the "publication of a photograph, film or recording of a person, which focuses on his sexuality, in circumstances in which publication may humiliate or denigrate the person, and in which the person has not granted consent for publication." Specifically, the amendment to the law is intended to deal with the posting of images, videos, or recordings of a sexual nature on social networks and via mobile messaging apps. The article states a five-year sentence for this offense. Guidelines published by the attorney general state that there is tangible public interest in enforcing the law against perpetrators, even in cases in which the suspects are minors and do not have a history of criminal behavior.[20] This is due to the serious harm caused by the offense and its far-reaching consequences for the victims and the need to make the criminal prohibition clear to youth.

In the case of online violence, law enforcement authorities have to deal with the phenomenon using the tools currently available in the criminal law. This requires the major actors involved—the police, the state prosecutor's office, and the courts—to exercise "creative caution"; that is, they must examine whether a particular act—only in new form—falls within the definition of an existing offense, or whether it breaks new ground and cannot be prohibited by existing criminal law. At the same time, these actors must exercise a degree of caution when applying criminal law to minors. This "creative caution" is a necessity for two main reasons: First, it is necessary to prevent the creation of an extra-territorial space on the internet where

19 Prevention of Sexual Harassment Law, 5758–1988.
20 State Attorney's guidelines 2.29

minors are abandoned and subjected to acts of violence by their peers. As described above, online violence breaks down the protective networks that defends minors, violates their private lives, and penetrates their homes, which are supposed to be their fortresses, and inflicts damage on several levels. The fact that children are unprotected inside their own homes and harmed in their own rooms, even under the watchful eyes of their parents, and that the harm caused is difficult to assess is not easily digestible. Minors should not have to walk about in fear, in neither the corridors of schools nor the internet. Therefore, even if certain difficulties may arise in proving that harm was done or in locating the assailants,[21] existing legal tools are sufficient in overcoming those difficulties, and it is imperative to act "creatively" in order to protect minors. The second reason "creative caution" is required is that this is a new issue, which is not yet completely understood; moreover, extra caution is required when dealing with minors and even more so when prosecuting them.

The question of the applicability of criminal norms in the virtual arena is a major issue; in many cases, the phenomenon of online violence does not, in fact, bring those norms into play. While in many cases, virtual offenses are committed online, obvious offenses are also committed in the real world but are broadcasted online. A simple example is that of a minor posting pictures of another minor in an intimate situation (for example, undressed) without their consent on a social network. In this case, while the photo was not printed and handed out to the minor's classmates, nature and substance of the act—publication that violates privacy without consent—does not change.

Some of the acts that constitute online violence are carried out in the real, physical world, and the internet serves merely as a means to immediately and simultaneously broadcast the act to the public; in these cases, the acts are not virtual acts, so the media through which they are distributed is of no importance. This becomes relevant primarily with regard to acts of online violence that violate privacy, but not only in such cases. One example is a situation in which several minors are holding a conversation in a chat room (or a WhatsApp group) and the inner dynamics of the group cause threats to be focused on one of the minors in the group. Unfortunately, minors threatening each other is commonplace both in the real and the virtual world,

21 One must bear in mind that anonymity on the internet is, in most cases, a mere semblance, and that most communications can be monitored by court order.

so the test should be the same in both worlds: Is it a "threat" as defined by law, and does it constitute a criminal offense that merits prosecution? The internet in this instance serves as a conduit for transmitting the threats instantly and simultaneously.

When police and prosecutors are informed about a suspected felony committed by a minor on the internet, they must ask themselves honestly: What is the difference from our perspective if the violent act was carried out on a social network, email, or telephone? The determining factor is not the mode of operation—virtual or real—but rather the nature of the act. When the essence of an action is a threat, a publication that violates privacy, or a provocation that borders on harassment, the medium makes no difference.

Actions performed by minors (for example, photographing a minor in his/hers private domain or hacking a minor's email) often have a tangible expression in the real world. This further reinforces the conclusion that there should not be a dichotomous separation between the real and virtual world. Furthermore, the connection between virtual behavior and damages in the real world is often seen in many areas. For example, a threat made on a social network can lead to a physical assault on a minor, and repeated harassment on the internet can lead a minor to commit suicide.[22]

The vast majority of abusive behaviors included in online violence seem to meet the definition of existing criminal law, and it may be inappropriate to separate between abuse online and offline. However, caution must be exercised before turning to criminal law in these cases. The *mens rea* that characterizes youth when engaging in online violence is unclear; sometimes it constitutes indifference to the hurt caused, and sometimes the injury results from recklessness as the boundary between social pressure, amusement, and the whims of youth on one hand and malice and the intent to cause harm on the other is blurred. A child posting something is not always aware to how widely his or her words can be circulated nor of their destructive power. Furthermore, the plethora of available media, together with the nature of social contacts between youths, means that the imposition of criminal liability may be disproportionate in some cases, even if we are talking about defending the same protected values—the reputation and the physical and mental health of the victim. The disproportionality stems from the fact that the youths may

22 See in other contexts criminal appeal 512/13 *John Doe v. State of Israel* (published in Nevo, December 4, 2013) Assaf Harduf, *Online Crime* (Nevo Publications, 2010) [Hebrew].

have acted on a whim and without being fully aware of the consequences of their actions. Furthermore, even if there are destructive consequences, it is possible that the assailant's original behavior was negligible but was blown out of proportion, due to widespread and rapid exposure to the action on the internet, as well as the provocative response.

It is relatively difficult for minors to commit the majority of criminal offenses in the real world, so the normative limits of permissible and prohibited, good and bad are thus more obvious. These boundaries, however, are much more blurred in the online environment, and as a result, it is more difficult to determine whether to conduct a criminal prosecution. Yet this does not mean that the online arena has been forfeited due to these difficulties; one should remember that committing criminal acts via email or on a social network, rather than face-to-face, does not diminish their severity, and to some extent this can even exacerbate them.

Conclusion

A minor's home is his castle and his mobile phone or computer are its extensions. A technological incursion into a minor's home does not necessarily have to be physical, and it can also be protected by the relevant criminal law. At the same time, defendants, both minors and adults, should not be allowed to take advantage of the accessibility and ease by which acts can be committed via the internet, which most likely they would not dare to commit face-to-face, as they would then constitute a criminal offense. The internet provides a sense of greater distance and protection when compared to a face-to-face situation and enables minors to traverse boundaries. The best way to prevent this is through education as to why this constitutes crossing boundaries and why it should not be done. However, criminal law should not ignore and enable the traversing of boundaries, and when necessary should have its say. Minors should not be allowed to commit acts that they would hesitate to commit in the real world, just because the internet provides them with supposed anonymity to conduct manipulations at the expense of their friends' emotional well-being and mental health; the internet must not become a sanctuary for committing offenses under the cover of anonymity and with the absence of physical contact. This is an obscene and unacceptable phenomenon that deserves more stringent criminal enforcement.

The distinction between words and deeds and between virtual behavior and real behavior is becoming more blurred. We have to be vigilant against creating a reality in which the virtual world, in the absence of criminal enforcement, provides a sanctuary for real criminals. The idea that violence must include physical contact needs to be abandoned. Minors can behave violently even without physical contact.

Furthermore, minors commit acts in the virtual arena that adults may be hesitant to commit, and there is often a need for an unequivocal response within criminal law against these deeds. Existing criminal legislation should be applied, with the requisite changes, in a way that not every obscene publication on the internet constitutes grounds for prosecution, such as in the case of defamation or violation of privacy. While the unique features of the internet discourse should be recognized, existing means should not be given up on *a priori* simply because of the challenges that this discourse entails.

The challenges that the virtual world poses require that law enforcement authorities adopt a cautious approach. In such cases, there may be room to request an opinion from the juvenile probation service prior to the indictment of a minor, regardless of age, in order to obtain a broader picture regarding the minor himself. Another possible solution is that the indictment of minors in such cases should be the responsibility of separate units within the police and the state prosecutor's office. Thus, a broad perspective on the issue will be formulated and application of criminal law will be fair and equitable. Furthermore, the tools that frequently serve minors could easily turn their conduct into such that could lead to imposing criminal responsibility—a situation the legislature surely did not imagine when attempting to define the violation of privacy or harassment. Giving this issue to an overall body that has a broad view will enable an ongoing and critical examination of whether criminal law is the appropriate tool to address this issue.

National Cybersecurity Strategies in the Healthcare Industry of Israel and the Netherlands: A Comparative Overview

Stefan Weenk

The rapid pace of society's technological innovations has created a set of transformative opportunities in the healthcare industry, notably elevating the quality of life while subsequently serving as a permeable arena for cybercriminals. The core function of healthcare is maintaining people's well-being and, in some cases, it constitutes a meaningful portion of national economic output. Growing cybersecurity risks to the critical infrastructure sector pose a threat to national security, prompting government response. This study compares the current national cybersecurity strategies and regulations used by Israel and the Netherlands to protect the healthcare sector against cyber threats and presents recommendations for future strategies and regulations.

Keywords: Healthcare industry, technology, national cybersecurity strategies and regulations, Internet of Medical Things (IoMT), critical infrastructure sector

Introduction

The healthcare sector has been one of the beneficiaries of the mounting technological advancements;[1] its purpose and operations are central to people's

Stefan Weenk earned a BA degree in Security Management Studies from Saxion University of Applied Sciences, Netherlands. He is a former research intern in the Cyber Security program at the INSS.

1 Sanjay Poonen, "Health Care Innovation Harnessing New Technology to Benefit Patients," *Forbes*, April 2, 2018, https://www.forbes.com/sites/forbestechcouncil/2018/04/02/health-care-innovation-harnessing-new-technologies-to-benefit-patients/#4d7afdf45a88.

wellness and, in some instances, representative of a significant portion of national economic output.[2] Emerging technologies and digitization play an instrumental role in the development of related products, services, and research, benefiting patients and providers. The integration of genetics and biology with big data and Artificial Intelligence—referred to as the "medical automation and information revolution"—has had an enhancing effect in research, revolutionizing drug production, personalized medicine, and clinical workspaces, and has altered the practical delivery of diagnosis and care.[3] Digitized health increases efficiency and effectiveness of medical systems, improving prescription management, remote healthcare, monitoring, and clinical operations.[4] Added value is further achieved by geographic scope, demonstrative of the Da Vinci Surgical Systems, or the use of robotic systems aiding surgeons to perform delicate operations from different locations.[5] The convergence of emerging technologies, information systems, and interconnected medical devices and networks, referred as the Internet of Medical Things (IoMT), is developed in disruptive and critical ways across healthcare systems.[6]

Cybersecurity Risks in the Healthcare Industry

A byproduct of the progress in digital health is the coinciding risk of IoMT and medical devices, as well as digital medical applications, software, information

2 "Health Care and Cyber Security: Increasing Threats Require Increased Capabilities," *KPMG* (September 2015), 1–6; "Critical Infrastructure Sectors," *US Department of Homeland Security (CISA)*, February 2, 2019, https://www.dhs.gov/cisa/critical-infrastructure-sectors; "Critical Infrastructure Sectors," *European Cooperation Network on Critical Infrastructure Protection (euconcip)*, March 15 2019, https://www.euconcip.org/; Lior Tabansky, "Critical Infrastructure Protection against Cyber Threats," *Military and Strategic Affairs* 3, no. 2 (2011): 61–78.

3 "2018–2019 Innovation in Israel Overview," *Israel Innovation Authority* (January 14, 2019): 60–62; Poonen, "Health Care Innovation Harnessing New Technology To Benefit Patients."

4 Deloitte Center for Health Solutions, *Connected Health How Digital Technology Is Transforming Health and Social Care* (London: Deloitte Center of Health Solutions, 2015), 1–40; "2018–2019 Innovation in Israel Overview."

5 Interview with Eliav N., November 25, 2018.

6 Safi Oranski, "Obstacles on the Path to Comprehensive IoMT Security," *Cyber MDX*, November 26, 2018, https://www.cybermdx.com/blog/obstacles-on-the-path-to-comprehensive-iomt-security.

systems, and security devices (firewalls and anti-virus).[7] Subsequently, these can jeopardize data, including organizational intellectual property, such as medical research, experiments, and findings; financial and billing information associated with electronic funds transfer (EFT); and patient information and medical history associated with electronic health records (her) or electronic medical records (EMR).[8] Ultimately, this will compromise the stability of healthcare operations and service delivery and will cause substantial cost in damages and settlements, harming the welfare of the people.[9]

To demonstrate the reality of the security weakness in medical infrastructure, researchers at Ben-Gurion University Cyber Security Research Center in Israel developed a malware that exploits vulnerabilities of medical imaging devices, such as CT and MRI machines, as well as the networks that process the scans. In the blind study, the altered CT scans—depicting cancerous nodes—deceived accomplished radiologists in misdiagnosing the conditions.[10] To the extent of public knowledge, this scenario has yet to transpire to the effect of directly causing injury or death. Most cyberattacks affecting the healthcare sector involve data breaches of electronic health records (EHR), caused by network vulnerabilities of hospitals, healthcare service providers such as insurance companies, and related supply-chain actors.[11]

---

7 Aurore Le Bris and Walid El-Asri "State of Cybersecurity & Cyber Threats in Healthcare Organizations Applied Cybersecurity Strategy for Managers," ESSEC Business School posted by Jean-Loup Richet on *Journal of Strategic Threat Intelligence*, January 10, 2017, https://blogs.harvard.edu/cybersecurity/2017/01/10/cybersecurity-cyber-threats-in-healthcare-organizations/; Barbara Filkins, *Health Care Cyberthreat Report* (SANS Institute and Norse, February 2014), 1–42; "Health Care and Cyber Security: Increasing Threats Require Increased Capabilities."

8 Le Bris and El-Asri "State of Cybersecurity & Cyber Threats in Healthcare Organizations Applied Cybersecurity Strategy for Managers"; Filkins, *Health Care Cyberthreat Report*; "Health Care and Cyber Security: Increasing Threats Require Increased Capabilities."

9 Le Bris and El-Asri "State of Cybersecurity & Cyber Threats in Healthcare Organizations Applied Cybersecurity Strategy for Managers"; Filkins, Health Care Cyberthreat Report; "Health Care and Cyber Security: Increasing Threats Require Increased Capabilities."

10 Kim Zetter, "Hospital Viruses: Fake Cancerous Nodes in CT Scans, Created by Malware, Trick Radiologists," *Washington Post*, April 3, 2019, https://www.washingtonpost.com/technology/2019/04/03/hospital-viruses-fake-cancerous-nodes-ct-scans-created-by-malware-trick-radiologists/.

11 Le Bris and El-Asri, "State of Cybersecurity and Cyber Threats in Healthcare Organizations Applied Cybersecurity Strategy for Managers"; Filkins, *Health Care Cyberthreat Report*.

An estimated quarter of all data breaches in the United States occur in the healthcare industry.[12] A notable case was illustrated by a new group of hackers discovered by Symantec in early 2015, referred to as Orangeworm. They deployed Kwampirs, a tailored malware targeting systems affecting computers of healthcare providers and third-party vendors across several sectors that provide services to the health industry, gaining unauthorized access to EHR and medical imaging devices, such as MRI and X-ray equipment.[13] In 2018, a phishing attack against staff email accounts at the Wisconsin-based UnityPoint Health resulted in the data breach of 16,000 patients, followed by a second attack on its business systems, resulting in the data breach of 1.4 million patients.[14] From 2015 to 2018, hackers targeted the Singapore state-health database, exploiting the records of 1.5 million patients including those of Prime Minister Lee Hsien Loong.[15] In 2018, the computer of an employee at the New York-based Med Associates, a healthcare billing claims vendor, was comprised, and more than 270,000 patients' records were exposed.[16] During the same year, the Missouri-based Cass Regional Medical Center, Blue Springs Family Care, and LabCorp were hit with ransomware attacks, preventing the use of their communication systems and EHR systems.[17] In June 2017, the computer networks of two to three hospitals were reportedly

12 Poonen, "Health Care Innovation Harnessing New Technology to Benefit Patients."

13 Jessica Davis, "New Hacking Group Targeting Healthcare Infects Mri, X-Ray Machine," *Healthcare IT News,* April 24, 2018, https://www.healthcareitnews.com/news/new-hacking-group-targeting-healthcare-infects-mri-x-ray-machine; Security Response Attack Investigation Team, "New Orangeworm Attack Group Targets the Healthcare Sector in the U.S., Europe, and Asia," *Symantec*, April 23, 2018, https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia.

14 Jessica Davis, "1.4 Million Patient Records Breached in Unitypoint Health Phishing Attack," *Healthcare IT News*, July 13, 2018, https://www.healthcareitnews.com/news/14-million-patient-records-breached-unitypoint-health-phishing-attack.

15 Jessica Davis, "Hackers Breach 1.5 Million Singapore Patient Records, Including the Prime Minister's," *Healthcare IT News*, July 20, 2018, https://www.healthcareitnews.com/news/hackers-breach-15-million-singapore-patient-records-including-prime-ministers.

16 Jessica Davis, "270,000 Patient Records Breached in Med Associates Hack," *Healthcare IT News*, June 20, 2018, https://www.healthcareitnews.com/news/270000-patient-records-breached-med-associates-hack.

17 Jessica Davis, "Update: Ransomware Attack on Cass Regional Shuts down HER," *Healthcare IT News*, July 11, 2018, https://www.healthcareitnews.com/news/update-ransomware-attack-cass-regional-shuts-down-ehr; Jessica Davis, "Ransomware, Malware Attack Breaches 45,000 Patient Records," *Healthcare IT News*, July 26, 2018, https://www.healthcareitnews.com/news/ransomware-malware-attack-breaches-45000-patient-records.

breached in Israel, although Israel's National Cyber Directorate confirmed only two, in fact, were attacked, resulting in the removal of fifty outdated and exposed computers.[18]

Regulation in the Healthcare Sector in Israel and the Netherlands

During the CyberMed seminar held at the Cybertech Tel Aviv conference in January 2019, the cybersecurity of the Israeli healthcare systems was deemed below par and unprepared for the pervasive threat to health communication networks, devices, and to the organizations as a whole. According to the director of Hadassah University Hospital, essential critical infrastructure is in compliance; yet for other elements, such as remote devices, the cybersecurity level is less resilient. The shift toward digital health propelled by emerging technologies and connectivity creates new challenges with a wider scope, threating the reputation of healthcare organizations.[19]

In comparison, in 2015, only 56 percent of the Dutch hospitals met the standards for information security in the healthcare industry (NEN-7510120).[20] Since May 2017, the measures have been binding and compliance has been a prerequisite across the healthcare industry in order to gain access to citizen service numbers.

The rising number of cyberattacks targeting networks and devices throughout the critical infrastructure sector endangers the utility and trust of healthcare providers and services. These attacks have led to initiatives to enhance the organizational resilience and robustness across the healthcare arena, including in organizations servicing the industry, and to amending a national cyber security strategy.

National Cybersecurity Strategies

Cybersecurity has materialized as an integral domain of organizational security, defined by the technology corporation CISCO as "the practice of

18 Globes Correspondent, "Cyber Attack Hits Israeli Hospitals," *Globes*, June 29, 2017, https://en.globes.co.il/en/article-cyber-attack-hits-israeli-hospitals-1001194803; Judy Siegel-Itzkovich and Sharon Udasin,"Cyber Attacks Hit Israeli Hospitals as Globe Battles New Computer Virus," *Jerusalem Post*, June 29, 2017, https://www.jpost.com/Israel-News/Israel-thwarts-hackers-from-cyber-attack-on-hospitals-498256.

19 Ami Rojkes Dombe, "CyberMed: Cyber Threats and Challenges in Healthcare," *Israel Defense*, January 28, 2019, https://www.israeldefense.co.il/en/node/37255.

20 CPB Netherlands Bureau for Economic Policy Analysis, *Cyber Security Assessment (CSRA) for the Economy* (The Hague: CPB Netherlands Bureau for Economic Policy Analysis, 2017), 1–41.

protecting systems, networks, and programs from digital attacks."[21] In 2011, "Ten National Cyber Security Strategies: A Comparison" was presented at the International Conference on Critical Information Infrastructure Security (CRITIS), wherein it described that "[at both the European level and] international level a harmonized definition of Cyber Security is clearly lacking."[22]

The formulation of national security strategies within the European Union is relatively recent and can be traced to the early 2000s. Establishing these strategies encourages policymakers to identify strategic objectives and provide a guide on how to reach those strategic objectives. A well-known statement in the security sector is that "cybersecurity is only as strong as the weakest link."[23] An organization can have the best cybersecurity structure, which can be, nonetheless, counter-productive without a comprehensive cybersecurity risk management system.[24] The cybersecurity evolution—the trail of events that catalyzed Dutch and Israeli cyber resolutions—requires clarification in order to understand the essence of both nations' current cybersecurity strategies. The strategy comparison will focus on how the Netherlands and Israel confront cybersecurity challenges and how both nations distinguish properties linked to cybersecurity policies.

The following criteria are based on the fundamental topics in the "NCSS Good Practice Guide"[25] and the research conducted by Luiijf and others[26] and will be used to compare the national cybersecurity strategies of Israel and the Netherlands. The first key issue is **risk governance at a strategic and national level**. One strategy of an organization is creating a wide-ranging master plan, which explains how the mission and objectives will be

21 "What is Cybersecurity," *CISCO*, December 2, 2018, https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html.

22 H.A.M. Luiijf, Kim Besseling, Maartje Spoelstra, and Patrick de Graaf, "Ten National Cyber Security Strategies: A Comparison," in *Critical Information Infrastructure Security*, ed. Sandro Bologna, Bernhard Hämmerli, Dimitris Gritzalis, and Stephen Wolthusen (Berlin: Springer, 2013), 1–17.

23 Niels Nagelhus Schia, "'Teach a Person How To Surf': Cyber Security as Development Assistance," *Norwegian Institute of International Affairs*, no. 4 (2016): 1–36.

24 Gabi Siboni and Hadas Klein, "Guidelines for the Management of Cyber Risks," *Cyber, Intelligence, and Security* 2, no. 2 (2018): 23–38.

25 European Union Agency for Network and Information Security (ENISA), *NCSS Good Practice Guide, Designing and Implementing National Cyber Security Strategies* (Heraklion: ENISA, 2016), 1–59.

26 Luiijf, Besseling, Spoelstra, and de Graaf, "Ten National Cyber Security Strategies: A Comparison."

achieved. The second key issue is the **national regulatory environment**, which is part of the overall national strategy of governments. The third key issue is major **stakeholders of the national cybersecurity strategies**. Moreover, this includes information about the landscape of the stakeholders, representative of multiple disciplines, who are involved in the process of developing the national cybersecurity strategy. The fourth key issue is the **definition of critical infrastructures and critical objects**. The final key issue **is cyber intelligence and cybersecurity awareness**. This section will expand on activities of cyber intelligence agencies and government bodies as they relate to resources availed to healthcare institutions and increasing cybersecurity awareness on a national level.

Risk Governance at a Strategic and National Level

The first key issue applied in analyzing a national cybersecurity strategy is risk governance. Risk governance offers organizations and states potential benefits and opportunities. Development of risk governance enables organizations and their environment to change while minimizing the negative consequences of the associated risks.

Risk Governance in Israel

Over the past decade, Israel's risk governance has shifted from its initial focus on the protection of computerized information infrastructures and databases prescribed by regulations to a more direct approach of protecting cyberspace with civil-military strategic interactions and public-private cooperation.[27] Although organizations face many challenges in cyber systems, academic and government programs are actively developing new operation and technical solutions that will improve the countermeasures and response to attacks.[28] In 2016, the National Cyber Directorate and the Ministry of Health implemented MedSOC, a security operations center for the medical industry. MedSOC probes attacks in the healthcare sector and publishes relevant information on its network; moreover, the portal is supported by

27 Michael Raska, *Confronting Cybersecurity Challenges: Israel's Evolving Cyber Defense Strategy* (Singapore: S. Rajaratnam School of International Studies, January 2015), https://www.rsis.edu.sg/wpcontent/uploads/2015/01/PR150108_-Israel_Evolving_Cyber_Strategy_WEB.pdf.

28 "Cyber Security Risk Governance," *International Risk Governance Council* (October 2015), 1–33.

the Computer Emergency Response Team (CERT-IL) under the National Cyber Directorate.[29]

Domestic regulation in Israel references international standards, in accordance to Government Resolution 2443 "Advancing National Regulation and Governmental Leadership in Cyber Security." Generally, all organizations are recommended or required to meet ISO/IEC 27001 and ISO 15408, the applicable standards for "organizational information security management systems" and evaluation measures for information technology security, respectively.[30] Designated organizations are required to meet additional measures based on national critical infrastructure criteria and the regulatory body. In 2012, the Ministry of Health issued Government Circular 18/2012, subjecting all healthcare organizations and associated service providers to comply with ISO 27799. It provided parameters in respect to the entity's "information security risk environment in selection, implementation, and management of controls," regarding "organizational information security standards and information security management practices."[31] The Ministry of Health has developed advanced healthcare certification together with the Standards Institution of Israel by adopting common criteria of other ISO standards.[32]

Medical equipment is manufactured with locked systems, hindering access to operating systems. Leading the National Cyber Directorate's medical research lab together with the Ichilov Hospital in quality regulations (government provided) testing of medical devices, the National Cyber Directorate provides knowledge and equipment, while Ichilov provides the

29 Interview with Eliav N., November 25, 2018.

30 Eli Greenbaum, "Israel Chapter on Cybersecurity – Getting the Deal Through," *Yigal Arnon & Co. Law Firm*, February 1, 2018, https://www.arnon.co.il/member/4358/articles; ISO/IEC 27001: 2013 Information technology- Security techniques- Information security management systems- Requirements," ISO, October 2013, https://www.iso.org/standard/54534.html; "ISO/IEC 15408–1:2009 Information technology-Security techniques-Evaluation criteria for IT security-Part 1: Introduction and general model," ISO, January 2014, https://www.iso.org/standard/50341.html.

31 Greenbaum, "Israel Chapter on Cybersecurity-Getting the Deal through," "ISO 27799:2008 Health informatics- information security management in health using ISO/IEC 27002," ISO, July 2008, https://www.iso.org/standard/41298.html; "ISO 27799:2016 Health informatics- Information security management in health using ISO/IEC 27002," ISO, July 2016, https://www.iso.org/standard/62777.html.

32 Interview with Yaniv P., January 6, 2019.

testing space. The assessments include a penetration test, network connectivity, and a vulnerability test.[33]

Risk Governance in the Netherlands

In 2018, in response to the opportunities and risks as a result of the digitization of the healthcare industry in the Netherlands, in addition to other challenges of data privacy and the Internet of Things (IoT),[34] Z-CERT was founded. The establishment was part of an initiative of the Dutch Association of Hospitals (Nederlandse Vereniging van Ziekenhuizen), the Dutch Federation of University Medical Centers (Nederlandse Federatie van Universitair Medische Centra), the Common Health Service Netherlands, and the Dutch National Cyber Security Center (NCSC). Z-CERT offers specialized services to healthcare institutions by providing in-depth knowledge of medical networks, applications, and devices.[35]

Medical devices must be assessed before admitted to the market, in order to determine whether the devices have been produced in accordance with the requirements of Directive 93/42/EEC and Directive 2007/47/EC regarding medical devices. Most of the development of medical devices is designed according to privacy and security principles, which means that the company that develops the medical devices has to pay attention to privacy-enhancing measures, also known as privacy-enhancing technologies (PET), as does the supply-chain vendors.[36]

Information security is the responsibility of the individual healthcare institution. The standards NEN 7510 and NEN 7512, which hospitals have to meet, ensure how information security and privacy can be achieved. Every hospital has to decide which standard best suits the risk environment of the hospital, with the exception of the statutory standards.[37]

The National Regulatory Environment

In order to regulate and reinforce cybersecurity measures in the healthcare industry, governments create regulations, requiring the healthcare industry to implement proper cybersecurity measures. Implementing regulations in

33 Interview with Eliav N., November 25, 2018.
34 Interview with Hessel B., December 17, 2018.
35 Interview with Hessel B., December 17, 2018.
36 Interview with Hessel B., December 17, 2018.
37 Interview with Hessel B., December 17, 2018.

the healthcare industry by placing the liability upon the organizations—as a result of rising lawsuits and fines for non-compliance by governmental agencies—creates greater cooperation.

Regulations in Israel

To ensure that public and private organizations can act upon cybersecurity threats, it is necessary to establish an (inter)national regulatory environment and/or an appropriate policy framework to frequently evaluate the strategies and objectives for cybersecurity and adjust them accordingly. Israel has implemented several privacy and cybersecurity protection laws since 1981 to deal with general privacy protection. Key regulations are the Privacy Protection Act of 1981;[38] the amended Privacy Protection Act of 2001;[39] Resolution 3611 of Advancing National Cyberspace Capabilities in 2011;[40] and Resolution 2444 of Advancing the National Preparedness for Cyber Security in 2015.[41] In 2018, the Israeli government published a draft in Hebrew of its cybersecurity law and issued a call for public comment. It represents years of consultation and debate concerning Israel's approach to cybersecurity and will combine cybersecurity legislation and policy with several new innovations.[42]

The Privacy Protection Act (PPA) constitutes the main regulation of Israeli data protection law. The law has two elements: The first is the general privacy protection and the second deals specifically with databases and is much closer to "informational" data protection law.[43] The PPA developed over time and has been amended nine times since it was first adopted in 1981. In 2001, the PPA introduced additional regulations, replicating European data protection terms and creating greater harmony with European standards.

The Israeli Law, Information and Technology Authority (ILITA) was created by government decision no. 4660 and established within the Ministry of Justice in September 2006. The mission of ILITA is to reinforce personal data protection, regulate the use of electronic signatures, and increase the

38 Ian Bourne, *A Guide to Data Protection in Israel* (Israeli Law, Information and Technology Authority [ILITA], January 2010).
39 Bourne, *A Guide to Data Protection in Israel.*
40 "Resolution 3611—Advancing National Cyberspace Capabilities," *Israel's Prime Minister's Office* (August 7, 2011), 1–6.
41 Deborah Housen-Couriel, *National Cyber Security Organisation: Israel* (Tallinin: Cyber Defense Center of Excellence NATO, 2017).
42 Bourne*, A Guide to Data Protection in Israel*.
43 Greenbaum, "Israel Chapter on Cybersecurity—Getting the Deal Through."

enforcement of privacy and IT-related offenses. ILITA also acts as a central knowledge base within the government for technology-related legislation and governmental IT large projects, such as eGov.[44] In 2011, resolution 3611 created the National Cyber Bureau (NCB), which was established to strengthen protection of critical national infrastructure, and regulate powers and responsibilities in the cyber realm.[45]

In 2012, the Ministry of Health published Circular 18/2012, which requires all healthcare institutions to obtain certification under ISO 2779. It also requires all service providers that hold either medical information or information regarding the infrastructure of the institution to comply with the standards of ISO 27799. [46]

Regulations in the Netherlands

To understand the Dutch national cybercrime and information security laws, it is useful to map the history of legislation leading up to the current (inter) national regulatory environment and/or an appropriate policy framework. With respect to cybercrime legislation in the Netherlands, the key regulations are the Computer Crime Act (Wet computercriminaliteit) of 1993[47] and the Computer Crime II Act (Wet computercriminaliteit II) of 2006; and the recent amendment resulting in the Computer Crime III Act.[48]

Informational privacy or data protection violations could be prosecuted on the basis of data interference (Article 350a of the Dutch Criminal Code[49]), but the Netherlands has no specification in its criminal law that specifically addresses data protection violations. The Data Protection Act (Wet bescherming

44 "Resolution 3611—Advancing National Cyberspace Capabilities."

45 Interview with Eliav N., November 25, 2018; Greenbaum, "Israel Chapter on Cybersecurity—Getting the Deal Through."

46 Deborah Housen-Couriel, "A Look at Israel's New Draft Cybersecurity Law," The Federmann Cyber Security Center Cyber Law Program The Hebrew University of Jerusalem (first appeared on Net Politics, published by the Council on Foreign Relations), August 5, 2018,https://csrcl.huji.ac.il/people/look-israels-new-draft-cybersecurity-law-new-draft-cybersecurity-law.

47 Government of the Netherlands: Ministry of Justice and Security, "Computer Crime Act" (October 28, 1993), 1–33 [Dutch].

48 The Government of the Netherlands: Ministry of Justice, "Computer Crime Act II," (July 4, 2006), 1–2 [Dutch]; The Government of the Netherlands: Ministry of Justice and Security "Computer Crime Act;" (October 8, 2018), 1–33 [Dutch].

49 "Dutch Criminal Code," *Official Publication of the Kingdom of the Netherlands* (April 22, 2015): 165 [Dutch].

persoonsgegevens) of 2000[50] is mainly enforced by administrative measures given by the government and was updated in 2015 to ensure that data leaks are reported by organizations and to extend the administrative power of the Dutch Data Protection Board (College bescherming persoonsgegevens).[51]

At the international level, the Netherlands, a member of the European Union, implemented the "Council Framework Decision 2005/222/JHA . . . on attacks against information systems" of February 2005. As a result of attacks against information systems and increased threats from organized crime, the European Union replaced the Framework Decision with "Directive 2013/40/EU . . . on attacks against information systems" in August 2013.[52]

The first EU-wide legislation specifically focusing on cybersecurity is called the Directive on Security of Network and Information Systems (NIS Directive). It provides legal measures to boost the overall level of cybersecurity and synchronizes cybersecurity policies between nations, ultimately to support the society and economy by enhancing digital readiness and minimizing cyber incidents. The preparation of the General Data Protection Regulation (GDPR) took four years before it was finally approved by the EU Parliament on April 14, 2016. The aim of the GDPR is to protect all EU citizens from privacy and data breaches. The main differences with the new GDPR and the previous directive are its extended EU-wide jurisdiction and fines for organizations that breach the GDPR regulations.[53] Designating a data protection officer (DPO) in the Netherlands is only mandatory if the organization meets the requirements of the GDPR. Each controller or processor is required to appoint a DPO if the organization is a government body or another public organization and in cases where processing includes (a) large-scale regular

50 "The Data Protection Act," *Official Publication of the Kingdom of the Netherlands* (July 6, 2000): 1–25 [Dutch].

51 "Amendment of the Data Protection Act," *Official Publication of the Kingdom of the Netherlands* (June 4, 2015): 1–8 [Dutch].

52 Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems," *Official Journal of the European Union* (March 16, 2005): 67–71; "Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA," *Official Journal of the European Union* (August 14, 2013): 8–14.

53 "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)," *Official Journal of the European Union* (May 4, 2016): 1–88.

and systematic monitoring of individuals, or (b) large-scale processing of sensitive personal data.[54]

Key Stakeholders of the National Cybersecurity Strategy

It is important to recognize the relevant stakeholders within the healthcare industry, as those who are involved in primary processes in the healthcare institutions. The all-inclusive national cybersecurity strategies of relevant stakeholders aid in achieving an optimized level of situational awareness, and in turn increase the yields of all strategy factors.[55]

Stakeholders in Israel

Israel is one of the pioneers of stakeholder cybersecurity cooperation among government institutions, academia, and private-sector organizations. Cybersecurity cooperation is a natural extension of the already-existing pattern of national cooperation in other areas,[56] and is reflected in one of Israel's flagship initiatives, the CyberSpark Innovation Initiative project in Be'er Sheva.

A multi-stakeholder process enables bringing together the appropriate and relevant actors. The context and scope of the strategy process, in particular the stage, helps significantly to determine the stakeholder profile. The organization responsible in this development of the national cybersecurity strategies in Israel is the National Cyber Directorate, involving stakeholders from three categories—the national sphere, civilian sphere, and national-international organizations—all relevant to the strategy's aim. The national sphere comprises government ministries and agencies that have knowledge and are associated with the healthcare industry, legislation, and cybersecurity. Stakeholders from the civilian sphere include the Israeli police and its national cyber unit, as well as academic entities. The national-international sphere includes the healthcare institutions, health maintenance organizations (HMOs), and international standardization organizations, among others.

Internal stakeholders include the chief information security officers (CISO), representatives from the IT divisions, and management in the

54 Global Legal Group, *The International Comparative Legal Guide to Data Protection 2018* (n.p.: Global Legal Group, 2018).

55 Alexander Klimburg, ed. *National Cyber Security Framework Manual* (Tallinin: NATO CCD COE 2012).

56 "A Look at Israel's New Draft Cybersecurity Law."

healthcare institutions. The Israeli healthcare industry is confronted with several international standards related to cyber information security; hence, it is beneficial to involve actors spanning branches of responsibility and knowledge within the framework of preparing a national cybersecurity strategy for the healthcare industry.

Stakeholders in the Netherlands

The Dutch cabinet created the National Cyber Security Strategy 2 (NCSS2) together with a wide range of public and private organizations, knowledge institutions, and civil society organizations. With the creation of the NCSS2, the government is shaping an integrated approach to cyber crime, which it announced in the coalition agreement.

On January 1, 2012, the Cyber Security Council (CSR) was formed in the Netherlands. The CSR is an independent advisory body composed of the Dutch cabinet and high-ranking representatives from public and private-sector organizations.[57] The Dutch government can depend on a wide range of public-private partnerships for the creation of a comprehensive and sound healthcare-related national cybersecurity strategy in the future. Two cooperatives, the Dutch healthcare-Information Sharing and Analysis Center (ISAC), and Z-CERT ensure that the healthcare industry is better protected by sharing information, ranging from cyberattacks across sectors and capability trends, among others.

Cyber diplomacy is another objective in the Netherlands' National Cybersecurity Strategy and aims to develop a hub for expertise on international law and cybersecurity. The hub will promote peaceful use of the digital domain and will bring together international experts and policymakers, diplomats, military personnel, and NGOs to share knowledge with existing institutes. International experts include those from the European Cybercrime Center 3 (EC3 – Europol) and Interpol Global Complex for Innovation (IGCI), which is a research development facility.[58]

57 Government of the Netherlands, "The National Cyber Security Center (NCSC) bundles knowledge and expertise," January 12, 2012, https://www.government.nl/latest/news/2012/01/12/the-national-cyber-security-center-ncsc-bundles-knowledge-and-expertise.

58 Annegret Bendiek, "The European Union's Foreign Policy Toolbox in International Cyber Diplomacy," *Cyber, Intelligence, and Security* 2, no. 3 (2018): 57–71.

Critical Infrastructures and Critical Objects

Understanding an organization's assets is not only necessary from a strategic business perspective but also from a (cyber) security perspective. Assets can be defined as tangible and intangible resources and capabilities that enable an organization to achieve its strategic objectives.[59]

Critical Infrastructure in Israel

The National Cyber Security Authority (NCSA) within the Prime Minister's Office, created the "cyber defense methodology for an organization" in June 2017. Protecting organizations within Israel is a component of its national defense concept, focused on protecting the Israeli economy and its vital components against any disruption. The NCSA's document supports organizations to define and map their assets, create risk assessment, and inspect their current cybersecurity systems. Israel's national cybersecurity strategy clearly focuses on mapping the critical and secondary assets of an organization and its links to suppliers. The supply chain is one of the greatest risks for an organization. As dependence on third-parties becomes increasingly critical in the healthcare industry, organizations are compelled to enhance and adapt their risk management processes.

A risk assessment of healthcare institutions conducted by the Ministry of Health revealed that some institutions depend on multiple systems supported by one external provider (third-party or supplier). The ministry also discovered that most of the Israeli hospitals are using the same system of this provider.[60] "The National Cyber Directorate is creating a healthcare-specific cyber strategy with a number of stakeholders to address the rising threat against cyberattacks in the healthcare sector," according to a representative from the agency.[61]

Critical Infrastructure in the Netherlands

The Dutch national cybersecurity strategy is developed to create a well-defined governance model with a dynamic balance between security, freedom, and social-economic benefits. At the same time, the Dutch government has tried to adapt the responsibilities that apply in physical security to cybersecurity

59 Mark Frigo and James Hurley, "Understanding Your Organization's Genuine Assets," *Strategic Finance,* February 2014.
60 Interview with Yaniv P., January 6, 2019.
61 Interview with Eliav N., November 25, 2018.

and intends to do that by creating a dialogue with organizations that deal with cyber threats. The Dutch government is currently not active in creating conditions and measures for the cybersecurity of supply chain of businesses or the healthcare industry, but a proposal for European legislation creates conditions and measures for ICT products and services.[62] Moreover, there is currently no healthcare-specific cybersecurity strategy to defend healthcare institutions against cyberattacks. From a national perspective, Dutch and European legislation, standards, and information protection authorities form the defensive layer.

Cyber Intelligence and Cybersecurity Awareness

In an effort to combat cyber threats and make organizations more aware of the risks, both Israel and the Netherlands focus on cyber intelligence and cybersecurity awareness in their critical infrastructure, as both nations have started to understand the objectives and effects of sophisticated and damaging attacks on the critical infrastructure.

Cyber Intelligence and Cybersecurity Awareness in Israel

The healthcare industry has not reached an optimized level of situational awareness in terms of the dangers for its networks and medical devices. In essence, negligence in addressing vulnerabilities and updating software makes healthcare institutions the perfect target.[63] Cyber intelligence for the healthcare industry is mainly delivered through government institutions, while the Ministry of Health collects cybersecurity information through a multitude of sources (i.e., government bodies, civic organizations, and international organizations).[64] The Ministry of Health has encouraged healthcare institutions to connect to its cyber intelligence services, free of charge, for extra protection.

Israel's MedSOC was created by the National Cyber Directorate and the Ministry of Health to provide information about cyberattacks in the healthcare industry and share information through the MedSOC network. Currently, MedSOC is connected only to hospitals, although it is expected

62 Interview with Tom S., December 19, 2018.

63 Patricia Williams and Andrew Woodward, "Cybersecurity Vulnerabilities in Medical Devices: A Complex Environment and Multifaceted Problem," *Dove Press Journal*, no. 8 (2015): 305–316.

64 Interview with Yaniv P., January 6, 2019.

to be connected to all healthcare institutions within the next five years.[65] Additionally, the Israeli government commits to fostering resources and efforts across educational institutions and to reinforcing cybersecurity efforts in the technology sector.

Cyber Intelligence and Cybersecurity Awareness in the Netherlands

Large organizations in the private sector in general are adequately focused on cybersecurity awareness, and most are aware that cyberattacks can cause damage to property; however, they can also damage the organization's image. The Dutch government has held meetings with other nations in the European Union to discuss if it should be mandatory for organizations to address cybersecurity for hardware and software.[66] Although the government has invested much in raising awareness for digital threats, a renewed approach is needed, focused more on stimulating and facilitating organizations to take action to improve online security. At the end of 2017, the Ministry of Economic Affairs and Climate Policy and the Ministry of Justice and Security jointly launched the "Digital Trust Center" (DTC) program. The DTC's mission is to increase the resilience of businesses to cyber threats with a focus on two key tasks. Its first task is to provide businesses with reliable and independent information on digital vulnerabilities and concrete advice on the action they should take. Its second task is to foster cybersecurity alliances between businesses.[67]

Comparative Findings

Both the national cybersecurity strategies of Israel and the Netherlands have similar aims of protecting cyberspace against their adversaries and enhancing cyber resilience. However, both countries' cyber threat landscape, socio-political conditions, security trends, traditions, the level of cyber awareness, among other components, have caused significant variations in the cybersecurity approaches of the two countries.[68]

---

65 Interview with Eliav N., November 25, 2018.

66 Herna Verhagen, *De economische en maatschappelijke noodzaak van meer cyber security—Nederland digitaal droge voeten* (The Hague: PostNL, September 2016).

67 Government of the Netherlands: Ministry of Economic Affairs and Climate Policy, "Factsheet Digital Trust Center," (August 6, 2018), 1–4.

68 Martti Lehto, "The Cyberspace Threats and Cyber Security Objectives in the Cyber Security Strategies," *International Journal of Cyber Warfare and Terrorism* 3, no. 3 (2013): 1–18.

Risk Governance

In terms of risk governance, the approaches of Israel and the Netherlands have many similarities and differences. Both nations have government bodies (in the Netherlands, the Ministry of Health and the NCSC; in Israel, the Ministry of Health, Welfare, and Sport, and the National Cyber Directorate) that organize regular meetings with healthcare institutions, aimed at maintaining industry knowledge and situational awareness, challenges, and relevant processes. However, with the creation of the MedSoc, which specifically supports the medical sector, Israel's government clearly shows it understands the present cyber threats are a potential danger to the business continuity of the healthcare industry. In contrast, the Netherlands has an operational National Cyber Security Operations Center, but there is not one specifically focused on the healthcare industry.

Regulatory Environment

In addition to the risk governance, the governments of Israel and the Netherlands have created similar cyber and information laws, but each country still maintains its unique composition based on the local and current situation. Both nations have developed regulations for appointing a CISO or DPO to an organization. Israel's Privacy Law requires data owners to appoint a data manager; although it is mandatory, it is not always enforced. Despite the similarities, there are some key differences. The Netherlands has a cybersecurity law currently modified to the GDPR, which created a better system for dealing with personal data and created the Data Protection Agency (DPA) as the main authority for this subject. Currently, Israel has no cybersecurity law (still in the drafting stage), making it difficult for government bodies to enforce certain cybersecurity measures or standards in the healthcare industry. Nevertheless, both regulatory environments regarding cybersecurity and information security are similar, since Israel has broadly replicated the European Data Protection Directive to bring about greater harmony with European standards.[69]

Key Stakeholders of the Strategy

Both countries are pioneers in cybersecurity as the Israeli and Dutch governments support cybersecurity cooperation among experts across the

69 Bourne, *A Guide to Data Protection in Israel.*

government institutions, as well as civil and industry sectors. Despite the fact that Israel's national cybersecurity strategy does not focus on international cooperation in the document, as in the case of the Dutch strategy, the multiple international public-private partnerships clearly indicate the government's interests in engaging international cooperation on this issue.

Definition of Critical Infrastructures and Critical Objects

A significant aspect in the national cybersecurity strategy of both nations is the confidentiality, integrity, and availability (CIA) triad of information. Israel's strategy emphasizes using specific controls to protect systems and organizations against harming the CIA of information and systems, whereas the Dutch document mainly mentions the CIA but does not provide any approaches on how to deal with cybersecurity. Both countries recognize that the critical and secondary assets of the healthcare institutions must be mapped to understand the threats to the processes and to understand the vulnerabilities in the healthcare systems.

Nevertheless, Israel's approach on dealing with the weak points in the supply chain of the healthcare industry is extraordinary in the cybersecurity field. Israel's National Cyber Directorate and the Ministry of Health have created a grade-based system to check how critical the supplier's systems or services are for the healthcare industry and to check the cybersecurity measures at the supplier, based on the criticality of the products and/or services.

Cyber Intelligence and Cybersecurity Awareness

Both Israel and the Netherlands are some of the more developed countries in terms of cyber innovation and cybersecurity measures. Israel's National Cyber Directorate proactively protects the healthcare industry by scanning the dark web on cybercriminals and new cyberattack methods. In the Netherlands, the intelligence service started the Joint SigInt Cyber Unit (JSCU), which provides information and expertise for the entire critical infrastructure. At the same time, the Dutch government has created a program to improve Dutch society's cybersecurity awareness through advertising and media. The initiative targets all Dutch citizens and the government is slowly changing its approach from that of being knowledge-based to having cybersecurity

skills.[70] In Israel, there is no such initiative to increase the cybersecurity skills of its citizens. However, the Israel Defense Force's Unit 8200 focuses on cyber warfare, acting as a catalyst for cybersecurity in the "high-tech" nation. Another difference is the MedSOC in Israel, which shares information about cyber threats specifically to the healthcare industry.

Conclusion

The technological changes in the healthcare industry and the ongoing threat of cyberattacks targeting healthcare networks and medical devices—amplified by greater connectivity—has created an expansive target, including IoMT, medical applications, software, information systems, and security devices across healthcare institutions. Given these growing threats across the critical infrastructure sector, many nations have developed strategies and regulations to enhance cybersecurity. The current Israeli and Dutch national cybersecurity strategies and regulations are comprehensive and take into account a multitude of cyber threats; however, both countries need to make some improvement in order to manage the ongoing cyber changes in the healthcare industry.

Risk governance in cybersecurity enables both countries to change and achieve their strategic objectives while risks are minimized. Both risk governance and the responsible ministries in Israel and the Netherlands focus on a bottom-up approach through cybersecurity meetings with directors and IT managers in hospitals. The approach to cybersecurity measures for medical devices differs considerably in both nations since Israel creates a safe environment to test the new medical devices before they are implemented in the healthcare industry, while the Netherlands chooses a more instructive way of advising healthcare operators to check their medical equipment before implementation.

Both countries have created regulations to protect data in organizations, including in healthcare, as well as private data of civilians against cybercriminals. Israel and the Netherlands created regulations for organizations to hire data managers (CISO or DPO) if they handle sensitive information. Another important law in both countries is the data notification breach law, which requires data managers to report data protection incidents. Israel, like the

70 Government of the Netherlands: Ministry of Justice and Security, *National Cyber Security Agenda: A Cyber Security Netherlands*, April 20, 2018.

Netherlands, eventually will implement a cybersecurity law, which will improve the handling of cybersecurity incidents.

Stakeholders strongly affect a country's national cybersecurity strategy since the operational level has a different view on cybersecurity than the strategic level. When governments want to improve the overall cybersecurity, employees of healthcare institutions benefit more from a respectable balance between cybersecurity and day-to-day work. Both Israel and the Netherlands interact on a regular basis with their stakeholders in the healthcare industry, in order to create effective cyber strategies that result in pro-active and multi-disciplinary commitment.

Alongside the process of formulating the critical infrastructure sector, healthcare institutions need to understand their critical and non-critical assets, so cybersecurity measures can be implemented specifically for safeguarding those assets. Both the national cybersecurity strategies of Israel and the Netherlands are focused on mapping organizations' assets through a process of risk assessment and inspecting current cyber defense systems. The confidentiality, integrity, and availability of information is the main concern for the healthcare industry, and both Israel and the Netherlands emphasize cybersecurity in order to prevent cyberattacks. A big difference between the two nations in supporting the healthcare industry is that Israel's government takes responsibility to help the healthcare industry with the vulnerabilities of the supply chain, while the Netherlands chooses to play a more informative role in the supply-chain security.

Finally, cyber intelligence and cybersecurity awareness are becoming a necessity of the healthcare industry. In Israel, the intelligence services work together with the Ministry of Health to scan the dark web on potential new cyberattacks. The Dutch military and general intelligence services created the National Response Network to detect and deter cyberattacks through new cybersecurity solutions. Furthermore, the Dutch government has designed a security awareness program using advertisements to inform of the dangers of the internet so that civilians will be more resilient. Israel has currently no similar program for cybersecurity awareness, but it increases the cyber knowledge through some IDF units, focused on cyber warfare and intelligence. Cyber intelligence in Israel is also spread through the new MedSOC in Beer Sheva, which allows the Ministry of Health and the National Cyber Directorate to upload information about cyberattacks or vulnerabilities.

Recommendations

This section consists of recommendations for the improvement and ongoing process of national cybersecurity strategies, partly based on the current strengths of the existing Israeli and Dutch strategies. First, the effectiveness of cyber strategies and regulations in both countries depends on the flexibility of the government in adapting to the evolving cyber domain. Future cybersecurity strategies should thus adhere to a basis of regulations in combination with reshaping the regulatory environment and information systems in critical infrastructure organizations in a flexible manner. Governments should update their strategies, policies, and regulations on an annual or bi-annual basis to keep up-to-date with new cyber advances.[71]

Second, an ongoing process of risk assessments is necessary to test and develop new cybersecurity strategies. Israel and the Netherlands should always maintain their cybersecurity approach to protect the healthcare industry against cyberattacks as cybercriminals will never stop trying to break into the information systems of healthcare institutions. Fortunately, both nations systematically test their cybersecurity strategies in national cybersecurity exercises to elevate and strengthen established security procedures. Israel's National Cyber Directorate and the Dutch equivalent, the NCSC, need to take more responsibility in the healthcare industry by encouraging institutions and their CISOs to create Business Continuity Plans and perform exercises to train staff in case of a cyber crisis.[72] In addition, to protect the national medical databases against cyberattacks, the Israeli National Cyber Directorate and Dutch Health and Youth Care Directorate should focus on smaller, less-secured institutions by creating a separate approach for them, as these institutions tend to be less eager or short-staffed to perform system updates or to buy new medical devices.

Third, the Israeli and Dutch governments should reference and explore the cybersecurity strategies of other cyber allies in order to ensure that the international threat landscape is handled as "many hands make light work." Within the cyber domain, this is exactly what is lacking at the moment between governments. Additionally, international consensus on definitions, regulations, and cybersecurity alternatives could alleviate regulatory constraints across nations.

71 Interview with Yaniv P., January 6, 2019.
72 Interview with Eliav N., November 25, 2018.

Fourth, more awareness of cybersecurity should be promoted in the healthcare institutions in particular and in the society in general. Part of the guidelines need to focus on cybersecurity awareness for healthcare staff, since healthcare staff is not concerned with it and rather is focused on the patient's health. Organizations and staff need to be aware of the cybersecurity dangers and attack methods.

Finally, although both Israel and the Netherlands have gaps in their cybersecurity approach, they both have a high-end approach to cybersecurity. Hopefully, future cyber research and additional effort in understanding the cyber threats in the healthcare industry will create a more resilient society in both countries. In addition, greater international cooperation with multiple countries across the world can make cyberspace a better and safer place.

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 twice 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:

Gal Perl Finkel and Gal Sapir
Coordinators, ***Cyber, Intelligence, and Security***
Tel: +972-3-6400400 / ext. 488
Cell: +972-50-7478315
galp@inss.org.il | gals@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 6997556 | Tel: +972-3-6400400 | Fax: +972-3-7447588