Cyber, Intelligence, and Security

Volume 2 | No. 3 | December 2018

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

Cyber, Intelligence, and Security

Volume 2 | No. 3 | December 2018

Contents

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

Cyber, Intelligence, and Security

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

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

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

Editor in Chief: Amos Yadlin
Editor: Gabi Siboni
Journal Coordinators: Hadas Klein and Gal Perl Finkel

Editorial Advisory Board

- Myriam Dunn Cavelty, Swiss Federal Institute of Technology Zurich, Switzerland
- Frank J. Cilluffo, George Washington University, US
- Stephen J. Cimbala, Penn State University, US
- Rut Diamint, Universidad Torcuato Di Tella, Argentina
- Maria Raquel Freire, University of Coimbra, Portugal
- Peter Viggo Jakobson, Royal Danish Defence College, Denmark
- Sunjoy Joshi, Observer Research Foundation, India
- Efraim Karsh, King's College London, United Kingdom
- Kai Michael Kenkel, Pontifical Catholic University of Rio de Janeiro, Brazil
- Jeffrey A. Larsen, Science Applications International Corporation, US
- James Lewis, Center for Strategic and International Studies, US
- Kobi Michael, The Institute for National Security Studies, Israel
- Theo Neethling, University of the Free State, South Africa
- John Nomikos, Research Institute for European and American Studies, Greece
- T.V. Paul, McGill University, Canada
- Glen Segell, Securitatem Vigilate, Ireland
- Bruno Tertrais, Fondation pour la Recherché Strategique, France
- James J. Wirtz, Naval Postgraduate School, US
- Ricardo Israel Zipper, Universidad Autónoma de Chile, Chile
- Daniel Zirker, University of Waikato, New Zealand

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

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

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

© 2018. All rights reserved.

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

Identity Theft and Exposure to Harmful Content—Internet Risks for Teenagers

Limor Ezioni

Children and teenagers are part of a weak and vulnerable population group. Their internet activity exposes them to two substantial risks: exposure to harmful content and identity theft and its use for slander and bullying. This article examines the characteristics and scope of the problem. It proposes ways of minimizing the damage that these risks pose to children and teenagers, while dealing with the existing privacy restrictions.

Keywords: Internet, internet bullying, identity theft, pornography, children, teenagers

Introduction

Technological development has many advantages but also more than a few disadvantages, ranging from society's absolute dependence on technology, which causes exposure to the shutdown of services and information leaks due to cyberattacks, to the possibility of financial fraud, and physical damage to critical processes. Despite the severity of these disadvantages, children and teenagers continue to be exposed to them, particularly to two dangerous phenomena: identity theft through the internet and exposure to harmful content.

Identity theft through the internet has become one of the main concerns in cyberspace, with teenagers being one of the most vulnerable risk groups.

Adv. Dr. Limor Ezioni, dean of law at the Academic College for Law and Science (Sha'arei Mishpat), is currently writing a book about cyber law and regulation. She provides professional legal counsel and representation in both criminal and civil law for teenagers and adults.

Identity theft and the use of false identities are, in many cases, aimed at slander and shaming campaigns, which are liable to have severe consequences for the teenagers whose identities were stolen, by affecting their future and their development. In addition to identity theft, children and teenagers are exposed to harmful content. Prolonged exposure to such content affects their social development, augments their violent inclinations, and is also liable to lead to the formation of distorted models of interpersonal relationships.

The information revolution, particularly digital communications on the internet, is based on leveling the differences between societies and cultures for the lofty purposes of educational, economic, and social development. The freedom to use the internet was a phenomenon that presumably promised social and economic development even in the most inaccessible places. Globalization ensued, in which information, knowledge, intellectual property, and capital were transferred quickly and easily between different countries. At the same time, the information revolution caused people to be dependent on the ability to transmit large volumes of various types of information at high speeds on diverse platforms.[1] The focus on—and some would say the addiction to—the ability to share information has repressed the need for controls over the content of the information. Under the banner of "net neutrality," the need and ability to exercise any control of content whatsoever has been suppressed. In theory, justice was on the side of the advocates of freedom who claimed and understood that this approach was likely to have desirable social effects even beyond the immediate benefits, such as those based on the desired externalities of net neutrality. In practice, however, the conditions justifying fair use of the internet do not exist in a place where the net neutrality model is in effect.[2] As a result, an unconstrained space has been created that allows the transmission of harmful content of any type whatsoever to any user.

In the absence of any control mechanisms by both the party distributing the information and the party receiving it, the internet has become a theater of lawlessness that victimizes mainly the weak. Teenagers and children are exposed to extremely harmful content, even against their will. The situation

1 M. F. Mahmood and N. Hussin, "Information in Conversion Era: Impact and Influence from 4th Industrial Revolution," *International Journal of Academic Research in Business and Social Sciences* 8, no. 9 (October 13, 2018): 320–328.

2 Keith N. Hylton, "Law, Social Welfare, and Net Neutrality," *Review of Industrial Organization* 50, no. 4 (June 2017): 417–429.

has become intolerable; in many cases, even an internet search for innocent content leads to pop-up windows with pornographic content inviting the user to enter a pornographic website. The inconceivable availability of this content makes it difficult for parents to cope with the phenomenon. Thus, without having any system of control, children and teenagers have become unwilling consumers of pornography.

As a weak and vulnerable population group, children and teenagers are subject to rapid manipulation and influence, creating a broad platform for another harmful use of the internet. The development of social networks has brought many benefits: Use of the internet can help create a widespread network of connections and colleagues with shared interests; the ability to distribute information on a large scale in a short period of time; and also the ability to market business services and products equally to everyone on a scale once only available to corporations with abundant resources. At the same time, the extensive use of the social networks has also caused problems: Identity theft, especially of teenagers, has become an affliction. The methods used to steal identities are highly developed and sophisticated, including penetrating an existing account, taking it over, and using it, or creating a fabricated account in the victim's name and connecting with his or her network of acquaintances. When teenagers are involved, the purpose is the same in most cases: posting and distributing malicious content in order to hurt the account's owner.

The key question arising in this context is whether ways can be found to minimize the two main risks for teenagers on the internet: the exposure to harmful content and identity theft, while also maintaining a balance between the need for freedom of information and privacy— the core of liberal democracy—and the need for better protection of children and teenagers.

Blocking Children and Teenagers from Harmful Content on the Internet

The idea that children have the right to protection when they are surfing the internet is a basic principle in a world that has an assortment of laws aimed at preventing abuse and exploitation on the internet. Nonetheless, the behavior of the content providers and the difficulty in instilling normative

surfing habits for children stretch the boundaries of protection and confront legislators around the world with new dilemmas.[3]

According to an article on the Global Kids Online blog,[4] the efforts to make the internet a safer place for children require creating a balance between developing digital skills among youth and devising a general policy for safeguarding the rights of children. The article showed that children begin using the internet at a young age and spend a great deal of time online. As a result, the likelihood of their being exposed to harmful content at an extremely young age has increased. The prevalence of smartphones exacerbates the problem and makes exposure possible at all hours of the day and night, including in situations where no parent or responsible adult is present. Moderate and judicious use of the internet can benefit children, but extensive and unrestrained use of it is liable to generate long-term negative effects on them. As children who lack skills in using the internet are apt to encounter educational and social difficulties, parents' attempts to restrict their use of the internet are liable to provide a doubled-edge sword and result in a destructive response. According to a survey conducted by the blog, 14 to 36 percent of youth between the ages of nine and seventeen have had a harmful experience on the internet.[5]

The United Kingdom has attempted to deal with this problem by a decision to create a mechanism for verifying the age to prevent youth from surfing on pornography websites. The British Board of Film Classification is responsible for implementing this mechanism. This approach is based on forcing broadband internet providers and cellular networks operators to block websites and applications that do not include means of identification for verifying the surfer's age. It is unclear, however, how an age verification system will be operated and what can be done to prevent it from being

3 Monica Bulger, Patrick Burton, Brian O'Neill, and Elisabeth Staksrud, "Where Policy and Practice Collide: Comparing United States, South African, and European Union Approaches to Protecting Children Online," *New Media and Society* 19, no. 5 (January 16, 2017): 750–764.

4 "Making the Internet Safer for Children: The Global Evidence," *Global Kids Online*, February 6, 2018.

5 Ibid.

bypassed without infringing on the surfers' privacy and without sharing personal particulars with providers of pornographic and harmful content.[6]

One of the operators of major pornographic websites, such as YouPorn, PornHub, and RedTube, proposed using a combination of a credit card, an SMS message, and passport or driver's license to verify the user's date of birth.[7] It appears that this method generates especially difficult privacy problems. In any case, as this essay was written, implementation of this mechanism had been postponed until a future date.[8]

Israel has also been dealing with this matter, including an attempt to enact a law blocking harmful content. A discussion has taken place for several months about ways of blocking teenagers' access to harmful content on the internet. A joint subcommittee of the Knesset Science and Technology Committee and the Knesset House Committee approved a bill along these lines in December 2018. The wording of the law allows internet subscribers to choose whether they wish to block their access to harmful content. Discussion of the bill, referred to as the "Pornography bill," focused mainly on two aspects. The first was the need to define the harmful content to be blocked, or more generally, the difficulty in regulating content on the internet, an area in which the state usually does not intervene. The second concerned infringement of privacy. The bill has been changed several times, but in general, it asks internet providers to send notices to subscribers, who will have to inform the providers whether they wish to activate a service that blocks harmful content.

In the discussion of the legislation, several points were raised, including the necessity of not treating all children in the 6–18 age range the same way, because it can be assumed that the damage caused by exposure to harmful content is not the same in every age group. The need to impose responsibility on providers of pornographic content, as well as on internet providers, also was discussed, including the suggestion that they place a warning panel with an age restriction across their website. At the same time, maintaining an open internet infrastructure free from censorship in order to protect the public's freedom was considered. It was also proposed to allow users who

6 Mark Jackson, "Age Verification and UK ISP Internet Porn Ban Quietly Delayed," *ISP News*, March 12, 2018.

7 Tom Allen, "PornHub's Age ID System Will Require Punters to Hand Over Their Date of Birth," *Inquirer*, February 1, 2018.

8 Jackson, "Age Verification and UK ISP Internet Porn Ban Quietly Delayed."

do not respond to the service provider's request that they agree to a content filter to continue receiving service without the filter being forced on them without their consent.[9]

The legislation, which requires companies providing internet services to respond to questions about blocking, will, in practice, create records making it possible to know which subscribers requested blocking and which said they did not want it. While the bill forbids the internet providers from using this information, the very existence of the record is liable to constitute a severe invasion of a person's privacy, especially when unauthorized parties could obtain the content of the records as a result of a malfunction or theft.

It is difficult to set clear and precise criteria for filtering material on the internet. As early as 1964, in a trial concerning freedom of speech, US Supreme Court Justice Potter Stewart said that he could not define pornography but was able to identify it by sight ("I know it when I see it"). Despite the difficulty, the large internet companies, such as Facebook, YouTube, and other internet platforms already filter content. It can be assumed that a public committee that will be formed will propose guidelines for facilitating the filtering of harmful content. These guidelines can be improved over time.

The main problem with the pornography bill remains that of privacy. Here technology that was developed for targeted advertising can help. The internet has materially changed the advertising market by facilitating advertising that focuses on predefined target markets. The major internet companies gather a great deal of information about internet users, including variables such as age, gender, language, location, family status, number of children, and so forth. This information is collected without the user's knowledge and stored for the purpose of building a profile that facilitates targeted advertising. For example, advertising for expensive school bags is published now only for parents with children of a specific age group living in certain areas, and who meet a particular income criterion. This technology is also used to conduct political campaigns before an election. In this way, specific messages can be directed to targeted audiences in every cross-section and segment.

The use of such technology for filtering purposes can be positive for children and teenagers. Using this technology, children in every age bracket can be identified on the internet, making it possible to immediately block

9 Gideon Allon, "'Porno Bill' Approved by Ministerial Legislative Committee," *Israel Hayom*, December 12, 2018.

content according to the users' age. The same method can also be used to establish filtering levels according to age group. For example, one filter can be used for the 5–9 age bracket, another for the 9–12 age bracket, and so on, instead of applying a general filter for all youth. This method will also prevent infringing on the users' privacy, because the filter will identify the user's group by its defined criteria and not the actual user.

No technology, however, is free from error. It can be assumed that cases will occur in which children are exposed to harmful content after this technology is applied, or in which adults will be blocked from such content. Experience from the advertising industry shows, however, that these exceptions are confined to a small number of cases. The use of the proposed technology will, therefore, substantially reduce the scope of the problem and facilitate a balance between the breach of privacy and other freedoms and the need to protect children and teenagers and allow them healthy and proper development.

Theft of Teenagers' Identities on the Internet

"Hi, Noa, we don't know each other, but someone is using your picture and has created a profile on Facebook." This was a notice received by Noa Benosh.[10] That is how Noa realized that an imposter was using her photographs on a fictitious Facebook account. Yariv (a pseudonym), a tenth-grade student, woke up one morning to discover that posts, which he had not written and pictures he did not know, had been posted on his Instagram account; someone apparently had broken into his account and posted malicious and humiliating content on it. He found himself trying to tell his friends in order to minimize the damage but with little success. Some were quick to respond, and some took advantage of the event to magnify the damage. These kinds of incidents are occurring at an increasing pace.

Social networks have become very popular. According to a report by Global Social Media Research, as of 2018, the number of social networks users worldwide was 3.2 billion, and this figure is growing at a rate of 13 percent a year.[11] The vast majority of youth have accounts on social

10 Noa Benosh, "A Person Suddenly Discovers that His Identity on Tinder Has Been Stolen," *Ynet*, January 12, 2018.

11 Dave Chaffey, "Global Social Media Research Summary 2018," *Smart Insights*, November 23, 2018.

networks, and 45 percent of them are almost constantly connected.[12] These figures are stunning in themselves. In addition to their popularity among youth, social media is also fertile ground for bullying as well as illegal and criminal activity. The main crimes on the internet, which are very common, can be divided into a number of categories: bullying and harassment, online threats, and identity theft for similar purposes. Table 1 below illustrates the scope of internet bullying in various countries (not including Israel), some of which results from identity theft and shaming campaigns and refers (in percentages) to parents who reported that their children had been exposed to bullying on the internet.[13]

Table 1. Percentage of Parents Reporting that Their Children Have Been Exposed to Cyber Bullying

Country	2011	2016	2018
India	32	32	37
Brazil	20	19	29
United States	15	34	26
Belgium	12	13	25
South Africa	10	25	26
Malaysia	–	–	23
Sweden	14	20	23
Canada	18	17	20
Turkey	5	14	20
Saudi Arabia	18	17	19
Australia	13	20	19
Mexico	8	20	18
United Kingdom	11	15	18
China	11	20	17

An analysis of the table shows the horrifying dimensions of the problem. The problem in Israel is presumably similar in scope as in other western countries (such as the United States, Sweden, and the United Kingdom).

12 Monica Anderson and Jingjing Jiang, "Teens, Social Media, & Technology 2018," *Pew Research Center, Internet and Technology*, May 31, 2018.

13 Sam Cook, "Cyberbullying Facts and Statistics for 2016–2018," *Comparitech*, November 12, 2018.

Youth make extensive use of the internet, but unfortunately, their judgment in response to the content posted on websites is extremely poor. They share many personal details without any control, including their full names, pictures, names of family members, telephone numbers, important dates, residential addresses, and so forth. All this constitutes a good platform for identity theft, which thieves can utilize to ostensibly make plausible posts. The level of security awareness among youth is also extremely low as they use unsecured wireless internet connections and usually employ the same passwords for different accounts. Many also share passwords not only with family members but also with friends.[14] The general impression among the public that youth are more aware than adults of the security problems on the internet is erroneous. In most cases, young people do not exercise basic internet hygiene, such as updating security measures and refraining from the disclosure of sensitive particulars on the internet. These phenomena make them easy prey for identity theft, both for the purpose of penetrating the social networks and for stealing identities of family members in order to commit fraud. A study conducted in the United States among 500 parents of children whose identity was stolen showed that the group with the highest risk of identity theft is the 12–17 age group (44 percent).[15]

What can be done about this problem? Identity theft and impersonation on the internet are a criminal offense in Israel under a number of laws. The Computers Law (1995) imposes a three-to-five-year prison term for one who "disrupts the proper operation of a computer or interferes with its use . . . deletes computer material alters it . . . performs an action with respect to information so it would result in the production of false information or false output . . . penetrates computer material located in a computer." The clause that is almost certainly relevant to the discussion here concerns an action resulting in false information or false output. In addition to this law is the Protection of Privacy Law (1981). Although this law concerns protecting a person's private information in databases, it is worthy to consider whether social media providers can be included in this definition. This would extend the responsibility of the major internet companies to the user's information,

14 Leigh, "Teenagers Are Easy Victims of Identity Theft," *Homeschooling Teen Magazine*, 2018.

15 Matt Tatham, "Survey: 12 Years Old is the Average Age of a Child Identity Theft Victim," *Experian*, August 26, 2018.

its security, and prevention of its use for fraud. Finally, the Prohibition of Defamation Law (1965) can be applied. Under this law, defamation is defined as something whose publication is liable "(1) to degrade a person (an individual or a corporation) before others or to make him the object of hatred, contempt, or ridicule; (2) to cause a person to be regarded with contempt for acts, conduct, or characteristics attributed to him; (3) to injure a person in his position, whether a public position or any other position, or in his business, occupation or profession; (4) to cause a person to be regarded with contempt because of his race, origin, religion, place of residence, age, gender, sexual inclination, or handicap." Impersonation on the internet and leaving malicious and humiliating posts can be subject to criminal charges and can also be considered a civil wrong entitling the victims to compensation.

It is difficult to determine how to reduce the exposure of young people to social networks, which sometimes amounts to an addiction. For this reason, in addition to relying on the law, other action should be taken. It is essential to teach young people how to behave on the internet, both in securing accounts and in selecting the content that they access, while helping them to realize the significance and consequences of sharing personal information on the internet. As it is impossible to completely eliminate the problem, in addition to these actions, it is also important to devote attention and provide assistance to the victims. A number of volunteer organizations have already begun moving in this direction.

The internet, social networks, and instant messaging applications create many positive opportunities to even out differences and provide equal opportunities. At the same time, however, the risks facing young people as a very vulnerable group are immense. We would be wise to create better and more sophisticated defense mechanisms for preventing attacks and bullying by impersonation. We should also demand that the major internet companies take more determined action to address these problems.

Conclusion

Children and teenagers are exposed to many internet risks and lack suitable tools for coping with them. This article analyzed two main risks: exposure of youth to harmful content and identity theft for purposes of humiliation, shaming, and slander. Various countries, including the State of Israel, have already begun taking steps in providing tools to minimize exposure of young

people to harmful content. The initial attempts, however, have encountered resistance from two main directions. The first is the argument that it is necessary to preserve net neutrality and avoid any censorship of internet content. The second is the difficulty in finding a mechanism that will prevent invasion of privacy. The mechanism proposed in this article can help solve the problem by blocking harmful content according to criteria of the internet users, as is already being done by the major internet companies in providing advertising services that target specific audiences.

Youth are not sufficiently aware of the possibility that their identity could be stolen and used for bullying purposes. For most of them, the risk of becoming a victim is usually intangible, and therefore they are unaware of the grave consequences posed by these incidents. Unfortunately, identity theft can destroy young people's ability to develop or critically injure them. It is advisable to adopt a multi-faceted solution to the problem of identity theft, by raising awareness among youth at risk, instilling suitable behavior on the internet, strictly enforcing the existing laws, and above all, aiding those injured by this affliction. This is only a start, however, as the damage suffered by young people on the internet can be significant. It is important and correct to expand the research around how to minimize and address this problem.

Ubiquitous Presence: Protecting Privacy and Forbidding Intrusion into a Person's Records in Jewish Law

Aviad Hacohen and Gabi Siboni

The development of internet use raises serious questions about a person's right to privacy and the duty of companies to safeguard the confidentiality of information they possess. In practice, too many events have occurred in which confidential information leaks out of the companies responsible for safeguarding it; such information is sometimes even sold to criminals. In the face of these abuses, the western legal system and regulatory agencies have been forced to deal extensively with this seemingly new issue in recent years. Yet, we find that this topic was discussed in some of the earliest sources of Jewish law. This article reviews this development, particularly given incidents in cyberspace in recent years.

Keywords: Privacy, Jewish law, cyber, online advertising

Introduction

Disturbing reports have been published recently about Facebook, the social network giant, and its use of the personal information of its members. Facebook has recently been the subject of negative publicity because of problems it has had in safeguarding the personal data of its users, as well

Prof. Aviad Hacohen is president of the Academic Center for Law and Science, dean of its School of Law, and director of its Center for the Instruction and Study of Jewish Law. Prof. Hacohen is a specialist in constitutional law and a research fellow at the Van Leer Jerusalem Institute. Dr. Col. (res.) Gabi Siboni heads the Cyber Security program at the Institute for National Security Studies.
The authors would like to thank Adv. Amy Yourman for her excellent comments.

as the way it uses their personal information in order to increase its income from targeted advertising. The problem, however, seems to be far more serious: Although Facebook proposes that a two-factor authentication be used to make it more difficult to steal the personal information of its users, this authentication system will require users to disclose their cellphone numbers to the company, which Facebook will then make commercial use of in order to bolster its own targeted advertising.[1]

Researchers have proved that Facebook systematically allows the use of identifying information, such as mobile phone numbers, for the purpose of targeted advertising aimed at cellphone owners. It does this without any transparency through saved user profiles, to which the users themselves have no access, and even worse, can do nothing about.[2] This means that even if a user does not want to be targeted by advertisers, the company will, nevertheless, still find a way to target the user and direct the advertising through a range of personal data.[3]

To paraphrase an ancient source, it can be said that "its presence is ubiquitous,"[4] meaning that there is virtually no hiding place from the discerning eye of Big Brother—the giant companies operating in cyberspace that use the information they accumulate with their tools. At the legal and moral level, this can be compared to a case in which the sinner profits,[5] instead of paying for his sin; not only is he committing a transgression, he is also being rewarded for it, as in, "have you murdered and also inherited?"[6]

Facebook is not the only culpable party in this matter; other companies are also using similar mechanisms, while the economic motive behind this is clear. When an advertiser wants to publish an ad, the advertiser tries to maximize the exposure of the product and display it to a targeted audience that is relevant to the product being sold. The large internet companies, such as Twitter, Google, Facebook, and others, follow this practice. They provide mechanisms for targeting the subject audiences and utilize the information

1 Lowell Heddings, "Facebook is Using Your Phone Number to Target Ads and You Can't Stop It," *How to Geek*, September 28, 2018.

2 Ibid.

3 Kashmir Hill, "Facebook Is Giving Advertisers Access to Your Shadow Contact Information," *Gizmodo*, September 26, 2018.

4 Tikunei HaZohar, Tekona 57, p. 92:72.

5 For example, see Baba Kama 38:72.

6 Kings 1:21:19.

gathered about the users. In most cases, the information is collected and utilized without the users' knowledge or consent.

The actions of these huge internet corporations violate the right to privacy, which is a basic principle of the concept of human rights. The essence of the right to privacy is a person's right to keep his or her life private and maintain a physical or virtual private space, which is exclusively controlled by that person and cannot be penetrated by anyone else without the person's consent. Some consider the right to privacy to be one of the "natural rights," such as the right to life and the right to human dignity and liberty, to which every human being is entitled. Others regard the right to privacy as part of a person's right to dignity, or as a means of exercising autonomy in accordance with the person's will.

The right to privacy is regarded by many as having been recognized relatively recently by human rights law, in comparison with other rights. They trace its origin to a seminal article, "The Right to Privacy," written by Samuel D. Warren and his law firm partner Louis D. Brandeis, later to become the first Jewish US Supreme Court Justice.[7] In it, the authors discuss the essence and origin of this right and extend it beyond a person's right to confidentiality of conversation and the right to protection from exposure of personal data and information (such as information about a person's health, economic circumstances, and past convictions for criminal offenses) to include a right to be left alone and in peace, without being unnecessarily disturbed against his will.

This basic constitutional right was established in Israeli law in Section 7(A) of the Basic Law: Human Dignity and Liberty, which states that no person can violate another's privacy without consent. The Protection of Privacy Law—1981 adds to this by stating, "No person shall infringe upon the privacy of another without his consent." Like other human rights, this right is not absolute. It can be qualified for reasons of state security, preservation of human life, safety and health, and so forth.

The right to privacy and the prohibitions in it constitute a large family of sub-rights and subordinate clauses. These include prohibitions on wiretapping, body searches, searches involving entry into a person's private premises, personal surveillance, perusal of personal documents without a person's

7 Samuel D. Warren, Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no. 5 (December 15, 1890), pp. 193–220.

knowledge and consent, penetration of a person's personal computer and its content, and so on. An examination of the sources of the right to privacy in Jewish law is likely to teach us that, the principles of maintaining a person's privacy and the right to an inviolate personal space are of ancient origin and can be used in our time as the basis for solutions for this issue.

Sources of the Right to Privacy in Jewish Law

Some are inclined to base the right to privacy in Jewish law on Balaam's prophecy in the Book of Numbers: "Balaam raised his eyes and saw Israel dwelling according to its tribes . . . and spoke in a parable . . . 'How goodly are your tents, O Jacob, your dwelling places, O Israel!'"[8] Although the context of this verse is a poetic prophecy by Balaam, who intended to curse Israel but gave a blessing instead, and not a normative-legal one that binds and commands (such as "Do not murder" and "Do not steal"), the verse was used by the ancient Jewish sages as a legal source for establishing the prohibition on infringing upon a person's privacy. In explaining what exactly Balaam saw that was "goodly" in "Jacob's tents," the sages said, "'How goodly' refers to his observation that they pitched their tents so that their openings did not face one another."[9] Balaam was thus praising Israel for what he regarded as scrupulous observance of the right to privacy.

The ban on infringing upon a person's privacy is specifically mentioned in Jewish law in many contexts[10] in which its importance is reflected, both through the commandment "Avoid evil and do good"—the obligation to prevent in advance any breach of privacy and the use of means of prevention—and through punishment after the fact. For example, the Mishnah states, "A person must not create an opening opposite an opening, or a window opposite a window. If his opening or window is small, he must not make it larger. If there

8 Numbers 24:2–5. It is interesting to note that this verse, spoken by a non-Jew—a Midianite prophet—was selected for the start of the Jewish prayer book and was placed at the beginning of the morning prayer recited every day. In our days, the "Voice of Israel" radio station began its daily broadcasts by quoting this verse.

9 For example, see Rashi, Numbers 24:5.

10 E. Lipshitz, "The Right to Privacy in Jewish Law and State Law," in *Parashat Hashavua*, vol. 4, ed. A. Hacohen and M. Wygoda (Jerusalem, 2012), p. 195; S. Aharoni-Goldberg, "Privacy on the Internet through a Halachic Prism," *Hapraklit* 52 (2013): 151–234.

is one opening, he must not turn it into two openings."[11] The Talmud asks, "What is the source for this? Rabbi Yochanan said, As the verse says, 'Balaam raised his eyes and saw Israel dwelling according to its tribes.' What did he see? He saw that the tent openings did not face each other and said, 'They are worthy to have the divine presence among them.'"[12] In his commentary on the Talmud, Rabbi Shmuel Bar Meir (Rashbam)[13] explains that the ban on creating a new opening opposite the opening to his neighbor's yard (or even opposite a yard shared by both of them) is designed to prevent damage caused by looking into another person's property; that is, infringement of another person's privacy.[14]

Eliahu Lifshitz states[15] that the Mishnah shows that damage to privacy caused by opening a window opposite a shared yard is **relative** and not **absolute** damage. For this reason, there is no requirement to conceal an existing window, even a large one; it is merely forbidden to create a new window or enlarge an existing one. If the window existed even before the neighbors moved in, they cannot force the window owner to change his situation; rather, they must take their own measures to prevent the infringement of their privacy. This ruling was summarized by Maimonides (Rambam) in his Mishnah Torah: "When a person has a window in his wall and a colleague comes and builds a courtyard next to it, the owner of the courtyard cannot tell the owner of the window: 'Close this window, so that you will not look at me,' for the owner of the window has established his right to maintain the window."[16]

Rabbi Gershom's Ban on Reading a Letter Without the Writer's Permission

Jewish law took a more significant step in protecting a person's privacy regarding personal documents—such as medical records, letters, and, nowadays, material stored on a personal computer—based on a *takanah*

11 Mishnah, Baba Batra Tractate, Chapter 3, No. 7.

12 Babylonian Talmud, Baba Batra, 60a.

13 Rabbi Shmuel Bar Meir (Rashbam) was a commentator on the Bible and the Talmud, one of the authors of the medieval Talmudic annotations, and a grandson and student of Rashi who lived in the first half of the twelfth century.

14 Rashbam, Baba Batra, 59b, 4:5 "Do not open."

15 Lifshitz, "The Right to Privacy in Jewish Law and State Law."

16 Rambam, Laws of Neighbors, Chapter 7, First law.

(Jewish religious ruling) by Rabbi Gershom ben Judah, the greatest Jewish sage in Germany in the tenth century. Among other things,[17] he declared a *herem* (communal shunning) against a person who reads someone else's letters without permission, as it invades the letter writer's privacy. The text of the herem reached us from a secondary source, among other things, because it was quoted in a book of responsa by Rabbi Meir from Rothenburg (Maharam),[18] who wrote, "There is a herem against looking at another person's letter, sent to a friend, without his knowledge."[19]

The herem declared by Rabbi Gershom was later confirmed and became a cornerstone of Jewish religious law, to the extent that many people wrote at the beginning of their private documents that the herem also applied to reading them. Some added "one who breaks a fence—a snake shall bite him;"[20] according to Rabbi Gershom, the letters of the Hebrew word for "snake" are an acronym for *nidui*, *herem*, and *shamta* (ostracism, shunning, and boycotting).[21] These expressions highlight the severity with which the sages of Jewish law regarded the invasion of privacy.

Reasons for the Ban in the Sources of Jewish Law

The Jewish law sages wrestled with the question of the source and reason for the prohibition on the infringement of privacy in past generations, many years before the article by Warren and Brandeis was published. Some scholars stated that an invasion of privacy unjustly enriches the person committing the infringement, at the expense of the person whose rights are violated. They believed that a person reading someone else's letters usually does so to gain an economic or other benefit by illegally using the other person's asset. Others regarded infringement of privacy by reading another person's writings as a form of borrowing without the owner's knowledge, an act

17 The most famous of his rulings were forbidding a man to divorce his wife against her will and a ban on polygamy.

18 Rabbi Meir from Rothenburg (Maharam) was a twelfth century Jewish sage in Germany.

19 Maharam from Rothenburg responsa, Part 4A, Section 22.

20 A verse appearing in the Book of Ecclesiastes 10:8. See the source in the preceding footnote for this custom.

21 Torat Chaim 3:47, *Talmudic Encyclopedia*, the entry "herem of Rabbi Gershom" (and in the online edition of the *Talmudic Micropedia*).

tantamount to stealing, which is forbidden even when committed for the purpose of fulfilling a religious commandment.[22]

Rabbi Chaim Palachi (Maharaf)[23] later extended the reasons for the prohibition in a different direction—to the "prohibiting" aspect rather than the "legal" aspect of Jewish law.[24] In his opinion,[25] opening and reading someone else's letter without that person's knowledge is the same as stealing "his conscience and deepest secrets." The violator thereby transgresses against the grave ban against deception. At the same time, Rabbi Palachi also cites the general and broad principle of the commandment, "love your neighbor as yourself,"[26] (which, as is known, the early sages interpreted in a negative form: "do not do to your fellow man what is hateful to you") as a possible source for applying the prohibition against infringing privacy.

Another scholar of Jewish law, Rabbi Israel Jacob Hagiz,[27] gave a different and interesting explanation for the prohibition on violating the privacy of a person's writings and stored information. He also held that the ban on looking at a person's records without permission came from the "prohibiting" aspect of Jewish law and was part of the stricture against gossip, one of the most severe prohibitions in Jewish law. He wrote that, "Another person's letter must not be opened, because it is forbidden to seek and search another person's secrets, and what is the difference between forbidding gossip for others or for himself?"[28]

Other scholars of Jewish law regarded this prohibition as being grounded in the prohibition on disclosing any information obtained from another person without that person's explicit permission. This view usually cites a ruling that appeared in the Babylonian Talmud: "Rabbi Musya, grandson of Rabbi Masya, said in the name of Rabbi Musya the Great, 'How do we know that, when one person says something to a second person, that the

22 Torat Chaim, ibid; *Talmudic Encyclopedia*, ibid.

23 Rabbi Chaim Palachi was one of the Jewish sages of Izmir in Turkey in the nineteenth century.

24 For the distinction between the "prohibiting" aspect and the "legal" aspect in Jewish law, see M. Alon, *Jewish Law* (Jerusalem: Magnus, 1988), pp. 100–124.

25 Rabbi Chaim Palachi, *Hikekei Lev*, Yoreh De'ah section, 49.

26 Leviticus 19:18.

27 Rabbi Israel Jacob Hagiz was one of the Jewish scholars in Fez, Morocco and later head of a yeshiva in Jerusalem in the seventeenth century.

28 Rabbi Israel Jacob Hagiz, Halakhot Ketanot, responsa, Part 1, 276.

second person cannot relate it to others without explicit permission from the first person? From Leviticus 1:1 —And the Lord spoke to him from the Tent of Meeting, saying.'"[29] Rashi commented that the word "saying" is a compound word—a kind of abbreviation, an acronym for "should not say," meaning that a person is usually enjoined from repeating things told to them by someone else unless given explicit permission to do so. If this is the case with something said directly to a person, it is even more valid with respect to something that was not directed at that person, whether it is written or spoken.[30]

Meaning of the Prohibition in the Information Age

Preserving the confidentiality of personal information is a basic duty of anyone possessing information of this type. The duty to conscientiously preserve the confidentiality of such information and adopt all reasonable measures to prevent it from reaching unauthorized parties applies to the major internet companies. In actuality, not only are these companies negligent about keeping the information confidential, as shown by recent cases of information leaked from Facebook as well as the recent disclosure that customers' data from the Marriott Hotel chain had been hacked,[31] but some make commercial use of the private information they possess and are taking steps to obtain information from other sources in order to promote their business. These companies compete for access to information in order to give those who advertise with them the opportunity to improve the targeting of their ads. They gather data from every possible source, including information about the viewing of internet pages, "like" clicks, the sharing of information, connecting via wireless networks, end-user device features, language, location, and dozens (some say hundreds) of other parameters. Data gathering is not confined to the internet; it is also spreading to the cellular space. For example, Android users who use Facebook's messaging application unknowingly provide their cellphone numbers to the company. Huge databases—private, public, military, medical, and commercial—contain enormous quantities of information that affect privacy, such as residential addresses, family status, CVs, and so forth.

29 Babylonian Talmud Yoma 4B.

30 Aharoni-Goldberg, "Privacy on the Internet through a Halachic Prism."

31 Brian Krebs, "Marriott: Data on 500 Million Guests Stolen in 4-Year Breach," *KrebsonSecurity*, November 30, 2018.

An employee or authorized person to whom confidential information has been given and who reads it or uses it without permission is a thief. This situation can open the door to civil damage suits against people or organizations who are negligent in preserving the confidentiality of the information they possess and who fail to implement all of the sufficient information security measures that a reasonable party like them should take. This also applies to an even greater extent to organizations that use this information in order to make a profit. In certain circumstances, such information security failure is also likely to constitute a criminal offense.

As noted above, the literature of Jewish religious law establishes various rules designed to protect the privacy of a person's documents. Some of these are determined by "avoid evil" statutes—whether by taking preventative measures before privacy is breached, or after the fact by punishing the party that has violated someone else's privacy. In other cases, infringement of the prohibition is combated by means of "do good"; that is, promising incentives and economic or spiritual rewards for a person who scrupulously avoids violating the privacy of others.

Given the severity of the prohibition, Jewish sages have ruled that Rabbi Gershom's herem, which bars opening or reading a document without its author's consent, applies even if the document is not labeled as confidential or classified.[32] In other words, reading a document without its author's express consent is forbidden. It is permissible only in exceptional cases, when it is intended for a worthy purpose (such as saving a person's life or in order to safeguard state security and public safety). Even then, it is permitted only proportionately, "to an extent that does not exceed what is necessary." In the opinion of one scholar of sage Jewish law, simply gaining access to another person's documents, even without reading them, constitutes a breach of Rabbi Gershom's herem.[33] This approach also has significant consequences for big data analysis by the major internet companies.

Maintaining privacy and the confidentiality of private information is not merely a technical matter; it has an exalted purpose. In the opinion of Rabbi Alfred Cohen, a person needs privacy, because privacy is the source and

32 See Palachi, *Hikekei Lev*, Yoreh De'ah section, 49.

33 Beit David, 14, 158.

means for realizing one's unique capabilities and talents.[34] Safeguarding the right to privacy is therefore not only a means of exercising other rights; it is also a value in itself as part of human dignity, as can be seen in Jewish law.

The general prohibition against infringing upon privacy as well as the specific prohibition against accessing another's records without that person's explicit consent are therefore deeply rooted in Jewish law. Accelerated technological development, the weaknesses of cyberspace, and difficulties in security pose new and exciting challenges to Jewish law concerning the application of ancient principles to our times—pouring the fine old wine of Jewish law into the new container of the legal system in Israel, whose values are both "Jewish and democratic."

34 Rabbi Alfred S. Cohen, "Privacy: A Jewish Perspective," *Journal of Halacha and Contemporary Society* 1 (1981): 57.

Cyberspace: The Next Arena for the Saudi-Iranian Conflict?

Ron Deutch and Yoel Guzansky

The combination of structural vagueness embodied in large cyber operations and their potential to cause real damage makes cyberspace the ideal field of action for Saudi Arabia and Iran and matches their strategic outlook and their concept of the use of force. The risk and the opportunity that cyberspace offers to each of these countries make it tempting, particularly when it concerns the long-term investment of resources. Cyberspace can therefore be expected to become another central arena of conflict between Saudi Arabia and Iran, given the limitations of conventional force.

Keywords: Saudi Arabia, Iran, cyber warfare, asymmetric warfare, Israel, United States

Introduction

Saudi Arabia and Iran have had a strong rivalry for some time. In spite of attempts over the years to reach a compromise, or, at least, certain strategic understandings to reduce the tensions between them, the two countries have continued to regard each other as a significant threat. Nonetheless, and despite their territorial proximity, they have never had substantial and direct military conflict between them but rather isolated clashes (especially during the Iran-Iraq war) and usually through third-party forces. The reason could be because of the nature of their armed forces and their operational concept. Historical, social, and geopolitical reasons have led to a situation

Ron Deutch is an intern at the Institute of National Security Studies. Dr. Yoel Guzansky is a senior researcher at the Institute of National Security Studies.

where neither Saudi Arabia nor Iran have ground forces that are able to perform extensive maneuvers beyond their borders, including against each other. Moreover, the Saudi army suffers from being extremely inefficient despite huge budgets, while the Iranians maintain an operational concept of their forces derived from a rationale of opposition and asymmetric warfare, as expressed by the central status and role of the Revolutionary Guards, and, in particular, the branch of the missile forces.[1]

Saudi Arabia and Iran's operational concept of the military force translates in theory into a broader strategic-political view, emphasizing psychological warfare and the use of terror and "proxies" under the radar in order to undermine their enemies. Perhaps it is possible to see a resemblance (whether rightly or wrongly) between this operational concept and the Gerasimov Doctrine, a relatively new concept in recent years that is gaining in importance as a potential approach to warfare and foreign policy in general.[2] Ascribed to the Russian General Valery Gerasimov, this doctrine is based on what he wrote in 2013, in which he described a kind of "new form" of wars. Alongside conventional military efforts, this new form included other channels of action, such as the use of the media, internal subversion, cyber, and any other means that can sow chaos in the enemy's ranks.[3]

This approach could acquire a particularly interesting angle when it is examined in the light of the development of cyber warfare. The combination of structural vagueness with the potential for real damage embodied in large cyber operations makes this the ideal field of action for Saudi Arabia and Iran's concept of the use of force. Thus, this article seeks to examine to what extent, if at all, cyberspace could become the main arena for the clash between Saudi Arabia and Iran. For this purpose, the article compares the cyber capabilities of each country, at both defensive and offensive levels, and tries to reach a conclusion as to whether cyberspace could provide one with the ability to achieve what they have failed to attain by conventional military means.

---

1 Uzi Rubin, "Missiles as the Flagships of the Iranian Regime's Vision," (Jerusalem: Jerusalem Institute of Strategic Studies, November 23, 2018).

2 Mark Galeotti, "I'm Sorry for Creating the 'Gerasimov Doctrine,'" *Foreign Policy*, March 5, 2018.

3 Molly K. McKew, "The Gerasimov Doctrine," *Politico Magazine*, September/October 2017.

Cyber in Saudi Arabia

The field of cyber did not attract much attention or consideration in Saudi Arabia until recent years. However, the kingdom's vulnerability to potentially dangerous cyber threats is constantly increasing. There are two main channels for potential damage. First is the "direct" channel, including possible attacks on both military and civilian infrastructures and facilities, which could lead to extensive economic damage, and even a high number of human casualties. A striking example of the destructive capability of this type of attack was witnessed in 2017, in the cyberattack directed at one of the Saudi Kingdom's petrochemical plants.[4] The purpose of the attack was not to steal information or harm Saudi databases but rather to cause real physical damage and an explosion that would disrupt the plant's systems. The operation failed due to an error in the attack code. Investigators believe that Iran was behind the attack, which has since corrected the error in the attack code, and now it is only a matter of time until it again acts against Saudi Arabia with greater intensity and sophistication.[5] Besides the focus on the threat to critical infrastructures and control systems that aim to interfere with the chain of supply and even cause physical damage, it is also possible now to identify a growing threat to information systems in Saudi organizations, for both disruptive and espionage purposes. At the end of 2016, several Saudi government targets were attacked, including the computer systems of the Central Bank of Saudi Arabia, by means of the Shamoon malware. This virus was first used back in 2012, in a large-scale cyberattack against Aramco, the Saudi national oil company. These examples are just some of the much larger series of attacks, hinted at by a senior figure in the Saudi cyber sector and who estimated that in 2015 alone, the kingdom had absorbed about 60 million cyberattacks, at a rate of about 164,000 attacks per day.[6]

In addition to the direct cyberattack channel, there is also the "indirect" channel, using the popular internet platforms such as Facebook and Twitter in support of elements opposed to the Saudi regime to ferment internal unrest. The advantage of this method is in the fact that it could have a much

4 Nicole Perlroth and Clifford Krauss, "A Cyber-attack in Saudi Arabia Failed to Cause Carnage, but the Next Attempt could be Deadly," *The Independent*, March 21, 2018.

5 Ibid.

6 Ibrahim al-Hussein, "60 Million Cyber-attacks Targeted Saudi Arabia in One Year," *Al Arabia*, May 2, 2018.

lower signature than direct cyberattacks, because of the attacking country's ability to disguise its activity as authentic internal protest, partly by using fictitious social media accounts. A combined action scenario should also not be ruled out: low signature cyber activity, causing a large civilian disaster that shocks Saudi society, combined with increased cybernetic subversion, exploiting the sensitive situation in order to encourage an active uprising against elements in the Saudi royal family.

The Saudi elite is beginning to understand the destructive potential of the cyber dimension and is trying to deal with it. At the same time, however, there are several internal factors that hamper these efforts. Above all, there is the structural split in the Saudi government, whereby the powers to deal with cyber strategy are divided between many power centers belonging to different ministries and organizations. This situation makes it difficult to draw up and implement a uniform cyber doctrine to meet the kingdom's various security needs.[7]

Another major obstacle that hampers Saudi efforts to deal with cyber threats is the relative technological backwardness of Saudi society. This problem is not new and is not unique to the cyber issue, but it touches on many of the deep ills affecting the kingdom. For many decades, oil wealth made it unnecessary to develop other economic sectors. The regime also "bought" popular acceptance through generous subsidies and a multiplicity of superfluous government posts, but, to a large extent, this deprived people of the incentives to work hard and acquire higher education. As a result, Saudi Arabia lacks the human and technology infrastructure needed to achieve the cyber capabilities it needs, including for civilian purposes, and is forced to rely on external help (information technologies account for only 0.4 percent of Saudi GDP).[8]

To try to overcome these difficulties, in recent years Saudi Arabia has taken a number of steps that have slightly improved the situation. Today it is possible to distinguish three major agencies in the kingdom operating simultaneously in the cyber field. The first is the National Cyber Defense Authority (NCA), which was established in 2017 by a royal order and is

7 Melissa Hathaway, Francesca Spidalieri, and Fahad Alsowailm, *Kingdom of Saudi Arabia Cyber Readiness at a Glance* (Potomac Institute for Policy Studies, 2017), pp. 23–24.

8 Ibid, p. 3

subordinate to the king and the crown prince. It is responsible for coordinating policy, guidelines, and training in cybersecurity for all government bodies, as well as private ones.[9] In essence, this is the organization with the overall responsibility for security technology in the kingdom. The second is the Saudi Federation for Cyber Security & Programming (SAFCSP), which is subordinate to the Saudi Olympic Committee and mainly responsible for preparing personnel and technological infrastructure for the cyber and programming sector in the country. Part of its regular activity is to organize conferences and competitions, in order to increase awareness of cybersecurity issues, encourage young people to specialize in this field, and serve as a potential technological reserve.[10]

While these two agencies operate openly, a third one is more attack-oriented and covert by nature, which, until recently at least, was reported to be run by Mohammed al-Katani, a close associate of Crown Prince Mohammed Bin Salman. This agency, the Center for Studies and Media (CSMA) in Riyad employs hundreds of Saudis who function as "an army of trolls" on social media channels, and their job is to monitor opponents of the regime, delete critical responses on sensitive matters, and post positive responses to Saudi royal policy.[11] Although many of its activities are carried out far from the spotlight of western media, the murder of the journalist Jamal Khashoggi put al-Katani on center stage together with the information war taking place under his direction, to which Khashoggi represented a significant threat.[12]

Notwithstanding the recent developments in Saudi Arabia in the field of cyber, it will take time to fully bridge the considerable gaps. Until the processes that were mentioned above gain momentum, Saudi Arabia will try to compensate for the gaps in its technological knowledge and infrastructure by purchases from other countries in the short to medium term. In the case of military procurement, Saudi Arabia is the largest customer of the United States, and the two countries have fruitful cooperation in the cyber field. The

9 "Follow Basic Cyber Security Standards, Govt Agencies Told," *Saudi Gazette*, October 7, 2018.

10 Official website of the Saudi Federation for Cyber Security and Programming, https://safcsp.org.sa/en.

11 Adam Goldman and Karam Shoumali, "Saudis' Image Makers: A Troll Army and a Twitter Insider," *New York Times*, October 20, 2018.

12 David Ignatius, "How a Chilling Saudi Cyberwar Ensnared Jamal Khashoggi," *Washington Post,* December 7, 2018.

MOU's signed by President Trump during his visit to Saudi Arabia in May 2017 included agreements on cybersecurity to help fill Saudi gaps in this area. It was also reported that contractors on behalf of the US administration are providing cyber defense consultation and training to Saudi Arabia and are also operating directly within Saudi ministries to protect them against cyberattacks. One of these companies, Booz Allen Hamilton, even felt it necessary to stress that its cyber involvement in Saudi Arabia does not include building offensive capabilities.[13]

The gaps in Saudi cyber capabilities could also influence its relations with Israel, which, as a cyber power, has a lot to offer the kingdom in this field. According to various reports, it is possible that such links already exist, or at least have existed in the past. In this framework, it was reported that parties connected to the Saudi regime had used the Pegasus spyware from the Israeli company NSO in an attempt to eavesdrop on its opponents.[14]

Another possible channel for Saudi Arabia is to create a shared cyber defense infrastructure jointly with the Gulf States under the Gulf Cooperation Council (GCC), or some of them, who face similar threats. Calls for such cooperation have already been heard, although the considerable tensions between some of these states mean that effective practical steps are still nowhere in sight.[15]

Iran's Cyber Capabilities

Unlike Saudi Arabia, Iran has a fairly well established infrastructure of cyber capabilities, both defensive and offensive. Iran's main targets of attack in recent years include Saudi Arabia, Israel, and the United States.[16] Iranian cyber activity is supervised at the highest levels of the regime, including the president and the commander of the Revolutionary Guards, and is maintained in several ways. First, the Iranian regime invests heavily

13 Michael Forsythe, Mark Mazzetti, Ben Hubbard, and Walt Bogdanich, "Consultants Stick with the Saudis," *New York Times*, November 8, 2018.

14 "Israeli Hacking Firm NSO Group Offered Saudis Cellphone Spy Tools – Report," *Times of Israel*, November 25, 2018.

15 Ramola Talwar Badam, "GCC Urged to Coordinate Cyber Security following Wannacry Attack," *The National*, May 21, 2017.

16 Collin Anderson and Karim Sadjadpour, "Iran's Cyber Threat, Espionage, Sabotage and Revenge," *Carnegie Endowment for International Peace*, 2018, https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf.

in research and training, based on a strategic perception of the importance of cyber.[17] Second, signing the nuclear treaty with the superpowers in 2015 opened up an opportunity for Iran to establish numerous opportunities for cooperation with universities and scientific institutes around the world. Iran exploited this opportunity to promote its cyber capabilities through working with institutions possessing the relevant knowledge.[18] Third, Iran's exploitation of foreign cyber knowledge is not limited to official cooperation. In 2013, Iran established the Mabna Institute, with the aim of gaining access to scientific resources from outside Iran.[19] While this goal is focused not only on the field of cyber, this is another possible channel with the potential to help Iran build its cyber capabilities.

Iran has certainly experienced the dangers embodied by cyberspace. The clearest example of this is the Stuxnet malicious worm that damaged Iranian nuclear infrastructures in 2012. But even before that, Iran had experienced cybernetic danger of another kind: The widespread protests in the streets of Teheran in 2009 illustrated the destructive potential of internal opposition groups and the flow of subversive ideas from outside. At that time, the Iranian regime started a project of isolating networks, with the aim of transferring all Iranian communication to an internal state-run network, cut off from the international arena, giving the regime full control of all content entering the country and better protection against cyberattacks.[20] This objective is backed by the Iranian "cyber police's" aggressive enforcement activity against subversive elements active on the internet.[21]

Apart from that, Iran invests extensive efforts in the development and assimilation of cybernetic capabilities, as well as practicing its operating

17 Gabi Siboni and Sammy Kronenfeld, "Developments in Iran's Cyber Warfare 2013–2014," *Military and Strategic Affairs* 6, no. 2 (August 2014): 84.

18 Levi Gundert, Sanil Chohan, and Greg Lesnewich, "Iran's Hacker Hierarchy Exposed: How the Islamic Republic of Iran Uses Contractors and Universities to Conduct Cyber Operations," *Recorded Future*, May 9, 2018.

19 According to FBI data, the victims of the Mabna Institute's activity include 3,768 professors in 144 universities in the United States alone, and 4,230 professors spread among 176 universities in 21 different countries, including Israel, Germany, China, South Korea, Britain, and Turkey. See Lior Tabansky, "Iran's Cybered Warfare Meets Western Cyber-Insecurity" in *Confronting an "Axis of Cyber"? China, Iran, North Korea, Russia in Cyberspace* ed. Fabio Rugge (Italia: ISPI, 2018), p. 130.

20 Siboni and Kronenfeld, "Developments in Iran's Cyber Capabilities," p. 85.

21 Ibid., p. 88.

concepts. Examples can be seen in the exercises carried out in 2012 and 2013, which tested respectively the Iranian cyber defense systems in the naval and ground forces of the Revolutionary Guards.[22] Recently, Iran has reported that it has discovered a more advanced version of the Stuxnet worm, although they claim that it has not yet managed to cause any damage. Following that, the head of the Iranian cyber system, General Gholam Reza Jalali, estimated that Iran was no longer under significant cyber threat and was therefore making the issue low priority. This report could indicate that Iranian cyber capabilities have been considerably improved, although this could be no more than psychological deception.[23]

While developing advanced defensive capabilities, Iran has also made impressive strides in the development of its offensive cyber arsenal. Iran is undoubtedly at a more advanced stage than Saudi Arabia in these capabilities, although it is apparently still lagging behind the large cyber powers like China, Russia, the United States, and Israel. The Iranian offensive cyber system is largely under the responsibility of the Revolutionary Guards and belongs to a sub-organization called the Iranian Cyber Army (ICA). This system suffers from a structural weakness due to its semi-contractual nature as most of Iran's cyber offensives are not carried out by Revolutionary Guards people but rather by semi-independent individuals and hacker groups, who are paid according to their success. In the absence of ideological commitment and the search for greater profits, many of these Iranian hackers become problematic candidates for the Revolutionary Guards. Consequently, the regime is adopting a multi-layered approach: At middle level management, they place officers who are ideologically committed to the regime, and they determine the objectives and assign tasks to ad-hoc sub-contractors; that is, groups of civilian hackers who are paid per task.[24] In addition, there are the cybernetic "proxies" who operate in a more ideological context. A prominent example is the Lebanese Hezbollah organization, whose ties to the Islamic Republic of Iran provide it with relatively advanced cyber capabilities in

22 Ibid., p. 87.

23 "Iran accuses an Israeli company of a cyber attack," *Jerusalem Center for Public & Political Affairs*, November 5, 2018.

24 Gundert, Chohan, and Lesnewich "Iran's Hacker Hierarchy Exposed," p. 5.

contrast to other terror organizations.[25] These capabilities are activated as necessary and represent a further cybernetic attack arm for the Iranian regime.

In addition, the Iranian regime activates its "soft" attack capabilities, namely the psychological warfare conducted by means of manipulating information on social networks and news websites, similar to what Saudi Arabia does. A prominent example of this capability— which was recently exposed—is an operation dubbed "Ayatollah BBC," a large-scale campaign on behalf of the Iranian regime in which news sites all over the world were faked, led by the Persian-language BBC site. The fake sites contained deliberately manipulative content, to meet the needs of Iran's psychological warfare.[26]

Conclusion

This article examined the feasibility of cyberspace developing into the next arena for widespread conflict between Saudi Arabia and Iran. In fact, cybernetic clashes between the two have already occurred, although this is not yet the focus of friction between them. Therefore, when discussing the Saudi-Iranian conflict in cyberspace, a distinction must be made between the short to medium term and the long term. As their experiences show, both these countries suffer from cybernetic weaknesses, which have the potential of opening them up to highly significant strategic damage. These weaknesses could turn out to be the cracks that bring down one of the two regimes, if one succeeds in landing a sufficiently severe blow. Since this is the case, the risks and opportunities that cyberspace represents for both Saudi Arabia and Iran make it tempting, particularly when it is a question of long-term investment of resources.

At present, it appears that the cybernetic capabilities of both these countries are too meager to cover full-scale conflict between them. They fulfill an important supporting role but are still insufficiently developed to provide a response for each country's security concept. Evidence of this can be found in the relatively simple means of aggression used by both Saudi Arabia and Iran in cyberspace. They include, above all, the dissemination of "fake news" and subversion through social media. Neither Saudi Arabia

25 Ben Schefer, "The Cyber Party of God: How Hezbollah Could Transform Cyberterrorism," *Georgetown Security Studies Review*, March 11, 2018.

26 "Ayatollah BBC – An Iranian Disinformation Operation against Western Media Outlets," *Clearsky Cyber Security*, 2018.

nor Iran possess wide-scale cyberattack capabilities; as far as it is known, Saudi Arabia still lacks independent technological abilities, and while Iran may be more advanced in this respect, it still relies to a large extent on semi-random "mercenaries."

The more interesting question that should be asked concerns the long-term trends. As already mentioned, decision makers in both Saudi Arabia and Iran are well aware of the potential for both damage and benefit inherent in cyberspace and are taking steps to position themselves as players in this field for the long term. To this must be added the strategic balance that the two have between them: neither Saudi Arabia nor Iran has the capabilities to defeat the other side using only conventional military means. This being the case, the decision to turn to the cyber channel—with the options it presents—is the obvious step. In this sense, we cannot rule out the possibility that we are seeing the first signs of a Saudi-Iranian technological race, in addition, of course, to all the cybernetic threats that separately occupy each of these two countries.

It is hard to predict the outcomes of such a race: On one hand, although it is possible to argue over Iran's status as a regular cyber power, at present Iran undoubtedly has an advantage over Saudi Arabia in this field. Iran has relatively well developed defensive infrastructures and valuable experience gained during the years of dealing with Israeli and American attacks. Also, unlike Saudi Arabia, which lacks real "hard" attack capabilities, Iran has demonstrated its ability to attack Saudi and western targets—American in particular—over the internet, even if it is apparently unable to mount a systematic and broad attack like Israel, Russia, and the United States. Finally, and above all, while Saudi Arabia is lacking technological and human infrastructure in the cyber field (or at most, only the first stirrings of such infrastructure), Iran has already invested extensive resources in providing university training and in working with foreign institutions, and even in stealing knowledge. All this has placed Iran several steps ahead of Saudi Arabia, and over time, this gap could become fatal for the kingdom.

On the other hand, there are two important factors that could work to the benefit of Saudi Arabia in the long-term technological race and block Iran's advancement. The first is the Saudi Kingdom's huge advantage in resources. The Saudi security forces enjoy some of the largest annual budgets in the world. If they are properly channeled and the smart investment in cyberspace

is increased, alongside those in advanced technological education, Saudi Arabia can accelerate its technological progress. Meanwhile, Iran, buckling under the burden of international sanctions, has difficulty in allocating similar resources to the development and acquisition of new capabilities.

Another important factor is the defense umbrella and the cooperation existing between Saudi Arabia and the world's largest cyber power—the United States. As a central ally, the United States can provide Saudi Arabia with the cybernetic defense umbrella and technological capabilities that will enable it to catch up with the Iranians. To this can be added what appears to be covert but frequent cooperation with Israel, which, as already stated, is a cyber power in itself. The relative weight of these benefits will increase as time passes. If they are wisely exploited by the kingdom, they could emerge as a real asset and give it a decisive advantage over Iran.

An examination of the current cyber capabilities of Saudi Arabia and Iran shows that a wide cybernetic conflict between these two countries is probably not imminent; however, the nature of cyberspace and its structural vagueness make it particularly suited to the way their concept of operational conduct. Therefore, in the medium-long term, we can expect both to make increased use of cyberspace as an additional way of damaging the enemy, in contrast to the limitations of their conventional forces, which have held them back until now.

Jihadi Johns: Virtual Democracy and Countering Violent Extremism Propaganda

Matthew Crosston

A growing body of literature documents how Islamic extremist groups utilize technology to recruit potential new extremists. This back-end analysis is not matched, however, by the equally important front-end part of the process: How and why do these virtual propaganda/recruiting tools work on populations living in Western societies? Why are people susceptible to extremism while living in stable, free democracies? This paper fuses elements of cognitive psychology (specifically Siboni's concept of the "first cognitive war") and virtual technology with the world of countering violent extremism to explain why Western counterterrorist organizations, from governments to the military to intelligence agencies, are having difficulty battling the virtual recruitment front. The overall failure of countering violent extremism (CVE) programs across Western democracies in the face of this virtual extremist onslaught will force some uncomfortable questions to the fore about how modern democracy in the digital age might be falling short of its ideals and civic promises, especially compared to the tech-savviness of radical extremists. This failure likely means the continuing success of extremist groups who advance violent agendas and kill more innocents. It also means the most advanced democracies will continue to lose the first cognitive war to extremist groups.

Keywords: Social media, internet propaganda, Islamic State, CVE, counterterrorism

Prof. Matthew Crosston is a member of the Senior Doctoral Faculty at the School of Security and Global Studies, American Military University.

Introduction

Although the Islamic State has not been able to maintain its physical geopolitical gains across Iraq and Syria, its ability to maximize its influence through various social media platforms in order to recruit people to commit atrocities in major Western metropolitan areas continues to be a disconcerting success. A growing body of literature documents exactly how Islamic radical groups utilize technology to ultimately recruit potential new extremists, but this back-end analysis is not matched by the equally important front-end part of the process: How and why do these virtual propaganda/recruiting tools work successfully on immigrant populations living in Western societies? Why are these people susceptible to extremism while living in stable, free democracies? This paper fuses elements of cognitive psychology (specifically Siboni's concept of the "first cognitive war") and virtual technology with the world of countering violent extremism (CVE) to explain why Western counterterrorist organizations, from governments to the military to intelligence agencies, are having difficulty in battling the virtual recruitment front.[1]

This article will address Western societies that have failed to psychologically integrate migrant communities into their democratic values. This lack of accountability to develop positive countermeasures is crucially causal as to why some groups are "in the West" but remain frustratingly not "of the West." How the internet seems to be a perfectly pernicious tool to exploit this failure of modern democracy's psychological promise will also be analyzed. The timeliness of this topic cuts across numerous important themes when it comes to the internet and society, including the role of social media in political campaigns and the formulation of intelligence policy; accountability and the rights of redress in the platform society; innovations (negative and positive) in civic participation and engagement; online social movements; instability and volatility in political life; and the rise of extremism and polarization.

This article will highlight an analysis of how extremist virtual propaganda works, relating to the effectiveness of the different types of virtual technology used and contrasting these techniques against the less efficacious and disappointing policies used by Western democracies to counter these groups. The overall failure of CVE programs in the face of this virtual

1 Gabi Siboni, "The First Cognitive War," in *Strategic Survey for Israel 2016–2017*, ed. Anat Kurz and Shlomo Brom (Tel Aviv: Institute for National Security Studies, 2016).

extremist onslaught will force some uncomfortable questions about how modern democracy in the digital age might be falling short of its ideals, especially compared to the tech-savviness of radical extremists. Failure to bring about this innovation likely means that extremist groups will continue to successfully advance violent agendas and killing more innocents. It also means the most advanced democracies will continue to lose the first cognitive war to extremist groups.

The Concept of the First Cognitive War

Siboni was the first to specifically coin the term "first cognitive war" in relation to the increasing use of virtual technology by sub-state groups to recruit actors to engage in a wide-range of activities undermining state welfare. Siboni highlighted how expansive these approaches were, ranging from engaging in academic and economic boycotts to undermining electoral and judicial legitimacy to committing physical acts of terror. In addition, he made explicit the efficacious use of virtual technologies to not only recruit so-called "lone wolves" to perform these tasks but also to make such incidents more spontaneous, less predictable, and requiring little to no formal organizational infrastructure or logistics.[2]

Siboni's original work focused exclusively on the immediate threat this capacity had on the proper functioning of the State of Israel. This article argues that the relevance of the first cognitive war concept extends far beyond the geographical territory of Israel and already has had a powerful impact on many advanced Western democracies across the globe. Perhaps most disconcerting is that Western consolidated democracies are not incorporating new counterstrategies to deal with this evolution in extremism. While the literature on cyber terrorism and the virtual recruitment of extremists is vast, as will be examined later in more detail, most of it details the method and logistics of the actual recruitment and the personal backgrounds of potential recruits. This means that a crucial aspect of the investigation is not being properly emphasized: the true "front-end" part of the virtual recruitment process, which tries to ascertain what has gone wrong psychologically and/or perceptionally for these recruits who reside in immigrant communities in Western democracies and who thus should be less susceptible to extremist propaganda.

2 Siboni, "The First Cognitive War."

This attitudinal aspect of potential recruits toward the democracies within which they reside is important because it speaks to the heart of the psychological foundation that might make them ripe for extremist recruitment. In some ways, this is the proto-battlefield in the first cognitive war: It matters how potential Jihadi Johns have experienced their initial foray of living in a proper democracy, and how this experience fosters a negative attitude about democratic institutions in general. Most important, counterterrorist agencies need to better understand this initial disenchantment because, arguably, it is only during this phase—which I call the pre-cursor phase—when governmental agencies have a legitimate opportunity to deter and stop the transformation of potential recruits into Jihadi Johns. The literature on cyber recruitment mostly has ignored this part of the process, having determined that any such critical perceptions about democratic society are largely *misperceptions* and thus not valuable to the overall investigation. This is erroneous. Since the entire point of the first cognitive war is about the ability of non-state groups to psychologically affect and influence individuals more powerfully than formal state organizations, the attitudinal positions of recruits about their host countries *before they are converted* do matter, and they matter a lot. Before diving deeper into this missing component, an overview of the literature on extremist recruitment is necessary.

Social Media, Cyber Jihad, and the Internet as Extremist Weapons

The idea of "electronic jihad" or "www.mujahideen" is not so new, as al-Qaeda first capitalized on it most prominently nearly twenty years ago. Thompson has critically analyzed how social media, which has become prevalent particularly among the millennial generation, has been dangerously effective at luring users in with promises of friendship and belonging. The virtual bombardment of radical messages could easily lead many unsuspecting recruits down a high-tech rabbit hole with no real knowledge of how to get out. Thompson showed how virtual penetration across various societies was actually well above average in the Middle East and North Africa, despite conventional Western impressions that these are backward regions. The Middle East even outpaced China's 31.6 percent virtual societal penetration, even though

most in the West consider China to be far more technologically advanced and savvy and its population overall far more connected to the internet.[3]

Keene elaborated on the connection between the internet and terrorist recruiters.[4] Acknowledging how difficult it is to not just monitor but also shut down radical internet sites and chat rooms, he recognized the power of the virtual media in positioning terrorist groups as purveyors of great causes and that the internet was a tool of empowerment in which potential recruits could be easily swayed to supporting positions far different from those of their host countries. Keene's work is emblematic of the early cyber-radicalism literature, where the positions and attitudes of potential recruits toward the host societies *before* they are exposed to extremist sites and propaganda are largely blank slates awaiting imprint. Elaborating on this space will help us understand the initial attractiveness of virtual radicalism among some Muslims living in the West. Indeed, Levin cataloged how during the early phases of virtual radicalization, the internet became a nearly fully-functioning ecosystem where American citizens (i.e., people who were born in America or naturalized after living for a long period of time in America, thus making it difficult to characterize this issue as an exclusively "other" problem) were fundamental in creating, maintaining, and propagating online content that would radicalize emigrant Muslims and even native-born Americans to carry out attacks on the homeland.[5] But once more, these overviews did not investigate the initial attitudinal state of potential recruits before their virtual exposure.

Of course, the key feature of the internet that gained so much approval by radical clerics has been its consistent fidelity. Unlike oral speeches or word-of-mouth, the internet allows someone to copy messages verbatim, send them literally all over the world without loss of any content, and give it a permanent virtual landing spot that people could return to or find no matter how much time has passed. Rudner recently extrapolated, in ascending order of severity, the multi-functionality of virtual activity by extremist Islamic groups:

---

3 R. L. Thompson, "Radicalization and the Use of Social Media," *Journal of Strategic Security* 4, no. 4 (2011): 167–190.

4 S. D. Keene, "Terrorism and the Internet: A Double-Edged Sword," *Journal of Money Laundering Control* 14, no. 4 (2011): 359–370.

5 Brian Levin, "The Original Web of Hate: Revolution Muslim and American Homegrown Extremists," *American Behavioral Scientist* 59, no. 12 (2015): 1609–1630.

1. subvert Muslim communities in Western democracies while deceiving and distracting
2. host governments from reacting to the threat at hand;
3. cultivate supportive attitudes toward acts of terrorism;
4. offer theological justification for acts of political violence and terror;
5. provide technical instructions and operational guidelines for terrorist acts;
6. promote direct involvement in preparatory activities that expedite terrorist operations;
7. encourage personal engagement in committing acts of terrorism. [6]

Works like this are focused more on the internal conversion element of recruiting. Indeed, Martin showed how virtual religious teaching played a greater role for recruitment than purely political philosophies, calling them the more necessary pre-cursor training. I argue the ultimate pre-cursor training for Western recruits is their process of disillusionment with Western society when initial migration came with high hopes and optimism. The literature needs a stronger focus on this process because, after all, it is doubtful that any amount of virtual recruitment would be successful if the "real-life" success of potential recruits in the West was substantial.

Gendron dug even deeper into understanding the nuances that were being used when producing a virtual call to jihad. These so-called grooming techniques employed a range of psychological, environmental, and social factors, each one with the capability of affecting individuals to varying degrees. Her study leaned heavily on the important work of the Center on Social Cohesion, which focused on three distinct core functions performed by jihadist websites:

1. ***Online libraries:*** Jihadist websites play a key role as repositories of lectures by keynote figures in the jihadi pantheon; videos prepared by al-Qaeda and other militant groups; and Nasheeds, traditional Arabic songs glorifying Islamic violence. Much of this material is made available online in English translations of the original Arabic sources;
2. ***Venue for preachers:*** Jihadist websites post sermons and tracts by prominent radical Islamist preachers and expositors of jihadism, which can be readily accessed through the internet;

6 Martin Rudner, "Electronic Jihad: The Internet as Al Qaeda's Catalyst for Global Terror," *Studies in Conflict & Terrorism* 40, no. 1 (2017): 10–23.

3. ***Forums for discourse:*** Jihadist websites usually host chatrooms, discussion forums, and newsgroups that facilitate e-conversations among like-minded followers and serve as organizational hubs for planning and coordinating activities addressing key issues. Social networking and media sites create and support online communities that enable jihadists and fellow activists to share information and reinforce bonding.[7]

Capitalizing on this work, Hamblet also utilized multiple expansive studies from Rand, the George Washington University, and the New York Police Department (NYPD), emphasizing that the Islamic State not only had deviated and had become more sophisticated in its internet usage over al-Qaeda but also that its recruitment bases were different, from geographical points of origin to overall average age. Perhaps most elucidative were the four stages of radicalization as identified in the NYPD report:

1. pre-radicalization: life before adoption of Salafi jihadist ideology;
2. self-identification: exploration into Salafi Islam;
3. indoctrination: intensification of beliefs, complete adoption of ideology;
4. jihadization: acceptance of the duty to wage jihad; planning and execution of attack.[8]

The NYPD report unfortunately does not provide equal analytical attention to each of the four stages. The latter three stage—self-identification, indoctrination, and jihadization—received far greater interest. As shall be seen later, the agencies and organizations most concerned with deterrence and countermeasures against radicalism have missed valuable opportunities by ignoring the pre-cursor stage; that is, life before adopting the extremist beliefs. Understanding why potential recruits can become so disillusioned with their host societies that they become ripe for extremist recruitment is a critical element most policing and intelligence organizations have still not analyzed deeply enough.

The importance of works like Gendron and Hamblet is that they show that internet technology has repurposed and rebranded this ideology— often portrayed by Western media and pundits as archaic, backward, and stuck in the sixteenth century—into something far more modern, charismatic,

7 Angela Gendron, "The Call to Jihad: Charismatic Preachers and the Internet," *Studies in Conflict & Terrorism* 40, no. 1 (2017): 44–61.

8 M. Hamblet, "The Islamic State's Virtual Caliphate," *Middle East Quarterly* 24, no. 4 (2017): 1–8.

and appealing. The present article requests, however, to remember that no matter how appealing or charismatic certain radical imams might be, and no matter how slick and attractive certain extremist websites have become, the style is not the sole factor in delivering individuals to jihadism.[9] The substance of what has gone wrong in the lives of potential recruits in the West (at least according to their own self-perception), which is subsequently blamed on the failure of Western society to deliver on its promises, is the crucial pre-cursor phase that needs to be amended in all of these fine works. Perhaps more important, it might be significantly easier to stop the path to jihadist ideology when it is in its embryonic stage rather than when it has already created card-carrying supporters of jihad. Aiming to virtually counter radicalism in the pre-cursor stage is logically more effective than countering it in the active adoption stages. This has been underemphasized in the literature to date and thus is missing from policy.

Picart comes close to exposing this gap when elaborating what was called "jihad chic" and "jihad cool." At first glance, Picart's investigation seems to be perfectly aligned with the principles of the first cognitive war and the need to understand the internal psychological processes of potential recruits. Ultimately, the inner desire to be relevant—a so-called "bad ass"—is deemed powerfully influential over young men as they are exposed to virtual recruitment.[10] While the stylistics of the actual recruitment—talking to potentials in the vernacular they understand and making radical behavior seem "cool"—is no doubt important, it still misses the essential pre-cursor element: Why would it be attractive to be a "bad ass" in extremist communities if a person already felt a "bad ass" in the majority host community? In contrast, in this article, I argue that it would not be attractive at all, and thus it becomes important to analyze the lack of integration success among recruits.

---

9 Anne Aly, "Brothers, Believers, Brave Mujahideen: Focusing Attention on the Audience of Violent Jihadist Preachers," *Studies in Conflict & Terrorism* 40, no. 1 (2017): 62–76; Peter Wignell, Sabine Tan, and Kay L. O'Halloran, "Under the Shade of AK47s: A Multimodal Approach to Violent Extremist Recruitment Strategies for Foreign Fighters," *Critical Studies on Terrorism* 10, no. 3 (2017): 429–452; Javier Argomaniz, "European Union Responses to Terrorist Use of the Internet," *Cooperation and Conflict* 50, no. 2 (2015): 250–268.

10 C.J.S. Picart, "Jihad Cool/Jihad Chic: The Roles of the Internet and Imagined Relations in the Self-Radicalization of Colleen LaRose (Jihad Jane)," *Societies* 5 (2015): 354–383.

Post properly framed the new dangers of this radical internet world, discussing how alienated individuals can be enticed into a "community of hatred."[11] Post also considered how even "homegrown" terrorism was a product of deliberate foreign outgroup strategies, making the necessary state counterstrategies incredibly difficult as they still had to honor Western principles of civil liberty and freedom. It is in this nuanced argument that we find a possible flaw: Works like this accurately acknowledge how easily Western counterpropaganda is dismissed but do not bother to ask why this dismissal is so de facto. If the potential recruits were enjoying the aforementioned civil liberties, freedoms, and advantages—the hallmark of the host democratic society—then counterpropaganda should *not* be easily dismissed, but it should not even be considered propaganda at all. Examining this disconnect is what keeps getting missed.

Moir built further on this community of hatred by looking at the revelation that radical social media sites were more than just communication venues; in fact, they were fundamental in building an isolated sense of belonging among recruits that would make them feel less attracted to or less enticed by anything offered in their native host countries.[12] While studies like these focus more on the process of indoctrination and on the seductive qualities offered through social media to potential new extremists, they do give credence to the argument made here that a competent understanding of how host communities failed to reach potential "lone wolves" is crucial to early and effective countermeasures.

Interestingly, some new emerging literature focuses on increased radicalization across the European Union and touches upon the pre-cursor factor. Macnair, Logan, and Frank have focused exclusively on the production of recruitment videos by the Islamic State's Al-Hayat Media Center. They rightfully emphasized that it was not just the professionally slick PR-type quality of the videos but also the highly emotional appeals embedded within the videos to groups already living in the West who are distraught or dissatisfied

11 J. M. Post, "Terrorism and Right-Wing Extremism: The Changing Face of Terrorism and Political Violence in the 21st Century: The Virtual Community of Hatred," *International Journal of Group Psychotherapy* 65, no. 2 (2015): 242–271.

12 N. L. Moir, "ISIL Radicalization, Recruitment, and Social Media Operations in Indonesia, Malaysia, and the Philippines," *Prism: A Journal of the Center for Complex Operations* 7, no. 1 (2017): 90–107.

with their lives there.[13] They ultimately focused on how the Islamic State videos sought to remedy that problem by promising joy, honor, and glory not just in this world but in the spiritual world beyond. This was actually something of a missed opportunity because the true level of potential recruits' susceptibility is not so much based on future promises as it is on dissatisfaction felt with their present countries.[14] Connecting from the promises of glory, they intimated that political indignation over perceived Muslim oppression was the flame that ignited their new radicalism. In contrast, in this article, I argue that instead of connecting to abstract grievances about global political repression, it is more logical and cogent that radicalization ignites within people who feel *personally aggrieved* by the countries within which they live. This feeling of disappointment about their individual success has been under-analyzed in terms of its counterterrorism value.

Brzica comes closest to aligning the existing literature with the aforementioned pre-cursor societal factor. Cogently linking together the decentralized and autonomous nature of the internet with the socially isolated characteristics of lone wolf terrorism, Brzica attested how difficult it was to figure out which sites—out of literally tens of thousands—deserved special deterrence attention and were more effective in creating real lone wolves motivated to carry out terrorist acts on Western soil.[15] Creating a category ranking of potential adherents to radical Islam, it is the fourth category that is most relevant to the present analysis: "migrants who have arrived to the EU, and who will potentially become radicalized due to their frustration with living conditions at their final destinations and in combination with

13 Logan Macnair and Richard Frank, "To My Brothers in the West . . . : A Thematic Analysis of Videos Produced by the Islamic State's Al-Hayat Media Center," *Journal of Contemporary Criminal Justice* 33, no. 3 (2017): 234–253.

14 Mohammed Hafez and Creighton Mullins. "The Radicalization Puzzle: A Theoretical Synthesis of Empirical Approaches to Homegrown Extremism," *Studies in Conflict & Terrorism* 38, no. 11 (2015): 958–975; Brian Levin, "The Original Web of Hate: Revolution Muslim and American Homegrown Extremists," *American Behavioral Scientist* 59, no. 12 (2015): 1609–1630; Guy D. Golan, "Countering Violent Extremism: A Whole Community Approach to Prevention and Intervention" (master's thesis, California State University 2016).

15 N. Brzica, "Potential Adherents of Radical Islam in Europe: Methods of Recruitment and the Age of Perpetrators in Acts of Terror," *Politička misao* 54, no. 4 (2017): 161–184.

exposure to radical jihadist propaganda online or via adherents of radical ideologies among established European Islamic communities."[16]

This is so close and yet still so far away, as Brzica analytically leaps forward to online propaganda and not backward to this "frustration with living conditions at their final destinations." By sticking with abstract concepts while ignoring more direct and explicit sources of local anger and aggression, the body of knowledge about lone wolf terrorism and extremist recruitment in the West remains tenuously connected to the first cognitive war concept. Indeed, Brzica's four categories of potential jihadists were given the following "vulnerabilities": socioeconomic status, cultural differences, sense of ethnic belonging (or lack thereof), religious convictions, and/or psychological factors.[17] While all of these factors clearly do play a role, mashing them all together with no distinction or analytical explicitness is conducting counterterrorism by throwing in the kitchen sink: it is accurate but relatively unhelpful for crafting deterrence strategies.

Greenberg's work is a wonderful archetype for the growing literature that is looking to determine if the internet, so effectively utilized as a tool for radicalization, can be equally utilized as a weapon for countermeasures. Unfortunately, this literature takes the internet as a form of deterrence too literally and focuses on potential solutions belatedly in the radicalization cycle. Greenberg, for example, focused on three main virtual techniques that might hopefully bear deterrence fruit: 1) Disruption efforts, which have relied on a series of technical interventions by internet companies on behalf of the US government; 2) Diversion and alternative engagement; and 3) the dissemination of counternarratives or countermessages.[18]

Overall, disruption has had little effect as the internet is an agile, highly adaptive technology. Even heavily autocratic regimes like China are incapable of simply "removing" radical transgressors through disruption. In many ways, diversion and alternative engagement goes hand-in-hand with countermessaging. Indeed, it is logical to presume that effective countermessaging should lead to alternative engagements for potential recruits. When it does not, the critique is always about the content of the

16 Brzica, "Potential Adherents," p. 170.

17 Brzica, "Potential Adherents," p. 170.

18 Karen J. Greenberg, "Counter-radicalization via the Internet," *Annals of the American Academy of Political and Social Science* 668, no. 1 (2016): 165–179.

countermessage. In other words, if a state can simply find the right message, the deterrence strategy will fall into place. The problem with this is that it fails to consider the crucial aspect of timing. Even the best countermessaging will prove ineffective when the potential recruit is too far down the extremist path. And since so much of state deterrence emphasizes trying to counter radicals long after they have been engaged by and recruited through online propaganda, it should not be surprising to learn that many of the deterrence strategies are engaged far too late in the process. In addition, these strategies do not draw a critical eye to possible societal culpability in creating a psychological atmosphere ripe for online recruitment. Greenberg notes that to date there is little confidence in countermeasure programs but that data and metrics still need to be properly cataloged and analyzed.[19] In the end, she remains optimistic that the internet can be used as a powerful tool to combat terrorism. I share that optimism, but only if the timing and self-criticism of Western governments becomes more acute when developing countermeasure strategies.

This extensive overview of the literature has shown a general failure to engage and analyze the lives and thinking of recruits prior to their full engagement with virtual radicalism. Rather than current tendencies to focus on heroic tales of glory, spiritual declarations of holiness, and abstract concepts of political resentment, I argue here that a more concrete estimation of frustration, despair, and general malaise produced by a failure to achieve success in the Western host country activates extremist attitudes among immigrant populations. Arguably most important for policy is the fact that if this is true, it actually gives states a better sense of *when* their countermeasure strategies need to be employed: when the potential recruits are both *in the West* and still hopeful to be *of the West*. Disrupting, diverting, and countermessaging when they are only in the West but no longer of the West is simply too late; it is a waste of state resources. A brief critical case study of the Tsarnaev brothers of the Boston Marathon bombing of 2013 will be used to explain.

The Tsarnaev Brothers: Frustrated American Dreamers?

The story of how two brothers, Tamerlan and Dzhokar, were caught for the Boston Marathon bombing is well documented. The process of how

19 Greenberg, "Counter-radicalization via the Internet."

Tamerlan slowly turned to charismatic Islamic imams online and got into trouble for domestic violence toward his American wife was covered with almost voyeuristic intensity.[20] While Dzhokar has often been characterized as the younger brother who simply idolized his older brother too much, the American public by and large felt no sympathy for him when given the death penalty.[21] In short, the Boston Marathon bombing case is largely a cautionary tale of how seemingly normal young men can inexplicably turn to radicalism even when given every opportunity in Western democratic society.[22] It was also mentioned numerous times how they were ethnically Chechen, as if this fact alone should have alerted local authorities to the potential danger when it came to Tamerlan and Dzhokar.[23]

This type of hindsight-oriented analysis in the aftermath of radical extremism is quite typical: Charismatic online Islamic preachers are just a religious interest until they are the source for radical brainwashing; being Chechen does not matter until it obviously means the spiritual essence of the brothers was always potentially violent; a man making his wife conform to strict Islamic dress codes is just being conservative until it means an overt rejection of Western principles of freedom. Even the details that documented their initial attempts to become more fully ensconced in American society were somewhat passed over, fleeting, superficial, and always doomed to failure.[24] I, however, think this type of analysis is missing the critical intervention period for effective extremist countermeasures and the important clues that help police, intelligence, and societal organizations in the first cognitive war.

The Tsarnaev brothers' case highlights how many opportunities exist for deterrence within the pre-cursor period. Tamerlan—who seemed the more athletic if also the less-educationally motivated brother—became quite serious in his pursuit of boxing, advancing far enough to represent the New

20 Peter Foster and Tom Parfitt, "Boston Bomber Arrested: Tamerlan Tsarnaev's Hateful Rage Behind American Dream," *The Telegraph*, April 20, 2013.

21 Ron Borges, "Dead Suspect's Coach: 'I Never Saw any Hatred'," *Boston Herald*, April 19, 2013.

22 Marc Fisher, "The Tsarnaev Family: A Faded Portrait of an Immigrant's American Dream," *Washington Post*, April 28, 2013.

23 Benjamin Lytal. "The Chechen Grievance: Tolstoy's 'Hadji Murad' After Boston," *Daily Beast*, April 21, 2013.

24 Peter Finn, Carol D. Leonnig, and Will Englund, "Tsarnaev Brothers' Homeland was War-Torn Chechnya," *Washington Post,* April 19, 2013.

England region in the National Golden Gloves Boxing Championships. During this time period he even openly stated that if his native Chechnya were to never gain independence and remain a troubled part of the Russian Federation, *then he would rather represent and fight for the United States at the Olympics* than be part of any Russian Olympic team.[25] In terms of the first cognitive war where virtual extremism is taking such a strong foothold, these kinds of statements are opportunities upon which to build. Tamerlan's resentment toward Russia is quite understandable to any member of the Chechen diaspora; but that resentment does not automatically transform into any desire to represent the United States. Any student of the Chechen wars knows that the Chechen "fight for independence" is just as easily characterized as a Russian conflict with radical Islamic extremism, given that the independence movement in Chechnya has been largely fueled by such extremist groups. Transnational Islamic extremism has always been equally dismissive and contemptuous of American and Russian societies, so at this early stage of Tamerlan's development it is clear he was still making a distinction between Russia (where his anger was more political than religious) and the United States (where he was clearly still willing to embrace his adoptive home country).

If anything, Dzhokar's foray into American life was even more immersive. Described as a friendly high school student who loved skateboarding and ultimately became captain of his school's wrestling team, Dzhokar would enroll at the University of Massachusetts at Dartmouth. While enrolled there he was outgoing, social, and well-liked, telling many people his ultimate intention was to become a dentist. This is again where most analyses of the Boston Marathon bombers simply dismiss Dzhokar as a weak-minded individual who was essentially powerless to stop his own brother's recruitment, subsequently following along out of familial loyalty. Whether this pop-psychological analysis is accurate or not is immaterial to the present work: What matters most is how obvious the opportunity was to intervene and deter Dzhokar during the pre-cursor phase. If anything, the younger brother was more immersed in American society than Tamerlan, looking to pursue the intensively socialized profession of dentistry. These

25 Snejana Farberov, "He Dreamed of Being an Olympic Boxing Hero for the USA but then Turned to Radical Islam; Older Bomb Suspect was a 'Talented' Fighter with a Dark Side," *Daily Mail*, April 20, 2013, p. 4.

opportunities should not be dismissed nor should the standard lament in such cases of extremism be affirmed: Counterterrorist agencies often believe potential recruits are only detectable after actively pursuing associations with radical groups. In reality, this is not always true. The Russian FSB in 2011 actually requested that the FBI look into Tamerlan as they believed during one of his recent family visits to the ethnic republic of Dagestan (which has its own longstanding history of Islamic extremism within Russia), he may have become involved with radical groups; alas, the FBI looked into it but found no credence to the Russian worry.

This shows that the current countermeasure model of seeking out recruit targets based on their dabbling with known extremist groups is too late and not effective in terms of discovering real threat agents. It certainly did not work with the Tsarnaev brothers. A program of proactive countermeasures based on positive immersion within the host society might have been more effective. It does not mean "fix" the Golden Gloves Boxing Championships so that Tamerlan wins or give Dzhokar an undeserved full scholarship to UMass-Dartmouth in order to become a dentist more easily. Rather, it means developing programs of interaction with those groups that come from "threat areas" like Chechnya but are aimed at helping them become even more successfully integrated into the local society. These types of programs exist across numerous Western democratic states for various groups and for many different reasons. Surely it is appropriate to add more programs on the principle of limiting the development of radical extremism at home.

These types of countermeasure programs would matter because in the case of the Tsarnaev brothers, it seems their radicalization was not spurred on by some innate anti-democratic, anti-Western hatred of American values. On the contrary, their radicalization seemed to perfectly coincide with the exact moment their American immersion paths started to go off the rails (Tamerlan's boxing future was stalled and Dzhokar's first year college grades put him in danger of academic probation). While he temporarily became something of a local celebrity with a single famous television interview, Ruslan Tsarni, uncle of the Tsarnaev brothers, explained rather simply that they were provoked to extremism by "being 'losers' and hating those who were able to settle themselves better."[26] This comment should have been taken more seriously; it intimated the critical tipping point of intervening

26 Finn, Leonnig, and Englund, "Tsarnaev Brothers' Homeland was War-Torn Chechnya."

at the moment when potential recruits are not yet enamored with extremist ideology but are nevertheless rocked by their own inability to "succeed" in their new homes. Assistance at this time period not only could be decisively effective in keeping potential recruits away from radicalism, it also would likely engender a deeper and more permanent sense of loyalty to the new home country, thus giving a greater layer of counterterrorist security. In a manner of speaking, it would be that rare instance of "positive profiling": assessing and pinpointing individuals for helpful intervention based on their backgrounds and heritage for increased security advantage. The effort to stop extremism as a "fallback option" for those who do not succeed needs to be the intervention/prevention focus for Western law enforcement and intelligence agencies. Pre-cursor intervention in the first cognitive war is about providing opportunity so that such fallbacks are seen as the poor choice that they truly are. Again, such positive interactions programs have long existed elsewhere for many diverse communities. It is time to let these programs work in the sphere of national security and intelligence.

Conclusion: The First Cognitive War Expanded

In February, the Program on Extremism at George Washington University released an eye-opening new report. *The Travelers: American Jihadists in Iraq and Syria* is a powerful mix of political science and sociology, exposing readers to American and European-based jihadist travelers. In the United States, evidence points to a loosely connected network of radicalization that dates all the way back to the early 1990s Balkan ethnic conflict. This provides further evidence of the "social balkanization" that has remained stubbornly prevalent with newer waves of emigrant populations. The George Washington University report acknowledges the feelings of isolation expressed among many new recruits in America but does not make a connection between this isolation and the clear failure of security communities to successfully integrate immigrants into American culture.[27] Understanding why some groups come to the United States but do not develop any great attraction to American political values could help law enforcement agencies ascertain who are the most susceptible individuals to such poisonous recruitment. As a whole,

27 Alexander Meleagrou-Hitchens, Seamus Hughes, and Bennett Clifford, *The Travelers: American Jihadists in Syria and Iraq* (Washington DC: Program on Extremism, George Washington University, 2018).

the American diplomatic community, the social assistance services, and the academics have not done an adequate job investigating the phenomenon best described as being "in the West" but never becoming "of the West."[28]

Unfortunately, Western governmental methods of counterterrorism may be growing antiquated as they continue to focus on the too-late phases of indoctrination and recruitment. If so, then the emergence of "Jihadi Janes and Johns" will not be marked by travel overseas or by direct personal contacts with known radicalized communities but rather will be frighteningly localized, hidden, and unpredictable. Until now, a patchwork of loose, radicalized elements, centered around well-known communities within major Western cities, have produced the most highly motivated recruits.[29] But as this work has evidenced, it is unlikely that this strategy of focusing on late-phases of indoctrination and recruitment will be highly efficient for preventing terrorism. Innovation in countermeasure strategy demands a new focus on the pre-cursor period to make progress in the first cognitive war, to discover recruits *before* they are recruited rather than *after* they have been well groomed.

This work is meant to hopefully fill a prominent gap in the literature: The analysis of radicalization and recruitment across the virtual space tends to be geared toward solutions that are also virtual. The argument here proposes, however, some of the best fighting tools against virtual radicalization are still housed within the social-psychological-cultural institutions and programs that can and should exist *in the real world*. After all, the pre-cursor phase is ideal for interventions that propose tangible results in the lives of potential recruits, not just esoteric e-promises. Very little research is presently making this connection. We should not fall into the trap that presumes virtual problems are best resolved only by virtual solutions. Besides, social assistance and law enforcement agencies both have advantages in terms of tangible programs and healthier financial budgets compared to distant radical groups reaching across the internet. These local social organizations must not turn their backs on one of the few areas in which they can prove more adept and be more directly participatory.

---

28 Matthew Crosston, "Jihad Selfie: The Evolving Strategy of Homegrown Radical Recruitment," *Homeland Security Today,* March 14, 2018.

29 Crosston, "Jihad Selfie."

Some prominent scholars long ago made explicit the issues of exclusion, isolation, and real-life difficulties of Muslims living in the West.[30] This article builds upon the shoulders of these scholars and shows the connection between these largely sociological revelations and the world of national security. Most importantly, it attempts to be a first step in revealing how that connection can elucidate new and innovative real-world strategies meant to reduce or prevent the development of lone wolf homegrown terrorism. This connectivity overall is currently lacking. Most distressing, this gap is not just about a missing niche in the body of knowledge; rather, it is about resultant policy lagging in its effectiveness to safeguard democratic societies from within the West itself. It is also about how policy is losing the battle over its own "brand"; that is, how individuals within susceptible migrant communities, new to the West and still fully impressionable, are not experiencing the ideals, values, opportunities, and advantages supposedly innate to Western democracy. This pre-cursor phase, where we connect the social-psychological-cultural to national security, is where we need to wage the initial forays in the first cognitive war. This is where the best opportunity for victory is found.

Siboni's original warning to the State of Israel to be more prepared and more adept for all aspects of the first cognitive war should be expanded, both in terms of states needing to get ready and the strategies that intelligence and political communities should employ to fight it. Producing innovation in the world of counterterrorism is not easy, especially when the argument here is to invest in "positive profiling" and proactively intervene in certain communities, and not to intimidate but to invest in group success. Another added benefit to this approach is that it makes no demands on private companies or commercial activity that might hinder virtual freedoms or limit overall societal access to the internet; rather, it demands that formal governmental agencies be at least as savvy and slick in its virtual engagement as extremist

30 Olivier Roy, *Globalized Islam: The Search for a New Ummah* (New York: Columbia University Press, 2004); Hale Afshar, "Islam, Globalization and Postmodernity," *International Affairs* 71, no. 4 (1995): 831; Carool Kersten. "Islam, Cultural Hybridity and Cosmopolitanism: New Muslim Intellectuals on Globalization," *Journal of International and Global Studies* 1, no. 1 (2009): 89–113; Akbar Ahmed, *Journey into Islam: The Crisis of Globalization* (Washington DC: Brookings Institution Press, 2007); Ali Mohammad, *Islam Encountering Globalisation* (London: Routledge, 2012).

groups are and as proactive in engaging potentials as the bad guys are. The important point to remember when facing the inevitable backlash to such proposals (because in the end groups will try to reframe this argument as "rewarding potential terrorists" or "bribing extremists to behave") is that this is where the efficacy of success will be highest, and where the impact will be greatest in terms of preventing successful recruiting and training. Moreover, these new pre-cursor period strategies will also have a secondary positive benefit of reaching deeper into communities that have traditionally been slow to embrace Western principles and tend to remain socially isolated from the ideas of civil liberty. Proactively breaking down this recalcitrant social balkanization by putting more duty upon the host country to invest in the success of these vulnerable communities is not "national security welfare"; rather, it is strategic domestic diplomacy aimed at winning the first cognitive war.

The European Union's Foreign Policy Toolbox in International Cyber Diplomacy

Annegret Bendiek

In September 2017, the European Union (EU) updated its 2013 Cyber Security Strategy. The new version is intended to improve the protection of Europe's critical infrastructure and boost the EU's digital self-assertiveness toward other regions of the world. To prevent conflicts from spiraling out of control in cyberspace, the EU agreed on a so-called Cyber Diplomacy Toolbox in October 2017, which sets out possible countermeasures in case of an external cyberattack and raises the costs for perpetrators. The framework encompasses the summoning of diplomats, further political, economic, and penal sanctions, as well as digital responses. However, the fundamental problem of attribution applies even to diplomatic responses. And since the use of the Toolbox is not only voluntary but also requires the unanimous support of all EU member states, there are multiple hurdles to a mount an effective defensive deterrence.

Keywords: Cyber, European Union, strategy, deterrence

Introduction

Ever since the cyberattacks against the computer networks of European governments and defense and foreign ministries have become public knowledge, security policymakers have insisted that the EU member

Dr. Annegret Bendiek is deputy head, EU/Europe Division, German Institute for International and Security Affairs Division, Berlin.

states need to develop more adequate cyber defense and cyber retaliation capabilities. However, the EU continues to base its cybersecurity strategy on the resilience of Information and Communication Technology Infrastructures and cyber diplomacy as part of its Common Foreign and Security Policy (CFSP) so as to position itself as a force for peace. Its Joint EU Diplomatic Response to Malicious Cyber Activities, adopted in October 2017, primarily stipulates non-military instruments that could contribute to "the mitigation of cybersecurity threats, conflict prevention, and greater stability in international relations."[1] Faced with increasing activities infrastructures, Europe's self-declared ambition is to adhere to the step-by-step cyber diplomacy plan, which is based on the principle of due diligence.

Cyberattacks, such as those against the information and telecommunications infrastructure of the German federal government,[2] cyber-espionage, intellectual property theft, cybercrime, or disinformation not only paralyze single communication and cybersecurity policies but they can also constitute part of hybrid warfare. "Hybrid" here means the deliberate covert or overt use of civilian and military instruments by state or non-state actors. Alongside cyberattacks, these include disinformation campaigns, espionage, economic pressure, the use of proxy forces, and other subversive activities. Therefore, after the nerve-gas attack in London, EU heads of government and state declared their unequivocal solidarity with the United Kingdom in late March 2018 and threatened Russia with consequences. Further sanctions are being considered, as is digital retaliation (hackback).[3] Within Europe, both the EU and the North Atlantic Treaty Organization (NATO) have focused their strategies on deterrence by resilience, although focusing on different strategic areas. A few cyber powers started to build up their offensive and defensive cyber capabilities. Likewise, the EU and NATO have begun corralling their respective members to establish common defensive capabilities; however, only a few countries within the EU and NATO, beyond the United States,

1 "Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities," 13007/17 LIMITE, *Council of the European Union*, Brussels, October 9, 2017, p. 2.

2 Thorsten Severin and Andrea Shalal, "German Government under Cyber Attack, Shores up Defenses" *Reuters*, March 1, 2018.

3 "Conclusions on the Salisbury Attack," *European Council*, March 22, 2018, http://www.consilium.europa.eu/en/press/press-releases/2018/03/22/european-council-conclusions-on-the-salisbury-attack/pdf.

such as the United Kingdom, France, Estonia, the Netherlands have the technical and legal capabilities to deploy offensive capabilities so far.

Cyber Defense: Defensive or Offensive?

It is a politically and legally controversial issue whether attacked states should adopt offensive countermeasures, such as hackbacks, to neutralize the source of a cyberattack. In its 2016 Cyber Security Strategy,[4] Germany pledged the need for defensive cyber security and called for the creation of a mobile Quick Reaction Force housed within the Federal Office for Information Security (BSI), as well as similar teams within the federal police and domestic intelligence agency that are able to respond to cyber threats against government institutions and critical infrastructure. The new coalition government takes the stance that the state requires military and strategic cyber weapons as well as a legal basis for their deployment in order to respond to cyberattacks, such as on the federal Parliament in 2015 or the government network in 2018.[5]

NATO categorizes attacks in cyberspace as a form of warfare, which can trigger the mutual defense clause under Article 5 of the North Atlantic Treaty. NATO is currently debating whether offensive computer-network operations by its member states should be a component of its operational planning. Since the 2016 NATO Summit in Warsaw, NATO-EU cooperation has been strengthened through the exchange of information and joint cybersecurity exercises. In its paper on German security policy and the future of the Bundeswehr from 2016, the German Defense Ministry extended this development and created a sixth organizational unit for its military—the cyberspace and information space unit—which currently has approximately 13,500 staff members.[6] In the case of self-defense or mutual defense within NATO, both defensive and offensive cyber defense capabilities may be used. Whether this holds true for offensive capabilities in peacetime is contentious. Critics argue that the proliferation of malware for cyberattacks does not justify the short-term advantages generated by the supposedly greater potential for

4 "Building and Community, German National Cyber Security Strategy," *Federal Ministry of the Interior*, 2016, http://www.bmi.bund.de/cybersicherheitsstrategie/.

5 Melissa Eddy, "Germany Says Hackers Infiltrated Main Government Network," *New York Times*, March 1, 2018.

6 "White Paper on German Security Policy and the Future of the Bundeswehr," *The German Federal Government*, 2016, https://bit.ly/2zXvJuE.

deterrence which these capabilities offer. They insist that confidence and security-building measures as well as arms control must be led by the United Nations (UN) and the Organization for Security and Cooperation in Europe (OSCE), and that any development of offensive cyber defense capabilities risks fueling mistrust, mutual insecurity, and conflicts. They believe that only a long-term cyber diplomacy coordinated at the EU level could help to bring about security in Europe and avoid conflict escalation.[7] Self-evidently, it is in the EU's own interests to position itself as building the norm in regional cybersecurity and to emphasize security and confidence-building measures in international cyber diplomacy.

Cyber Diplomacy Formats

Cyber diplomacy—as opposed to overall cyber defense—offers the potential for conflict de-escalation and thus for developing a force for peace. More than thirty states now have commissioners for cyber foreign policy. Denmark has even appointed a cyber diplomacy ambassador. Cyber diplomacy in the widest sense encompasses confidence-building measures (CBMs). It also comprises certain aspects of international norm building, data protection, freedom of expression, internet governance, and prosecution under international agreements for not providing mutual legal assistance. Many governments, however, have neither the knowledge nor the necessary resources to maintain basic cybersecurity standards or even to ascertain attacks that are being conducted via servers on their territory. Nevertheless, most states voice profound reservations over national sovereignty when presented with the idea of a central global regulatory body for security in cyberspace, thereby rendering it an unrealistic prospect for the time being. More likely, cyberspace and information space will be increasingly subject to national sovereignty.[8] Meanwhile governmental regulation will always lag behind the technical development in the private sector. Public-private partnerships is therefore the predominant mode of regulation in cyber security.

---

7 See André Barrinha and Thomas Renard, "Cyber-Diplomacy: The Making of an International Society in the Digital Age," *Global Affairs* 3, no. 4–5 (2017): 353–364; André Barrinha, "Virtual Neighbors. Russia and the EU in Cyberspace," *Insight Turkey* 20 no. 3 (2018): 29–41.

8 Milton Mueller, *Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace* (Polity, Cambridge, UK, Malden, MA 2017).

On the multilateral level, in 2015, a group of twenty-five international government experts commissioned by the UN General Assembly reached a consensus that international law should be applied in cyberspace as well, including the right to self-defense.[9] However, in summer 2017, the group could not agree on whether to establish a so-called attribution council. As a precondition for attribution—meaning the technical, legal, and political identification of the perpetrator of a cyberattack—sensitive information must be exchanged among Computer Emergency Response Teams (CERTs) and between secret services and security agencies.

Due to ineffective multilateral formats, Presidents Xi Jinping and Vladimir Putin signed a bilateral joint declaration in 2016 in Shanghai announcing a new phase in the comprehensive strategic partnership between China and Russia. Beijing and Moscow voiced their concern that information and telecommunications technologies were being misused for interference in internal affairs. The international community, they stated, should cooperate on the basis of mutual respect and expediency as well as justice, and provide joint responses to threats to information security.[10] The United States also relies on bilateral agreements, for instance with China, to fight cybercrime.[11]

Ever since multilateral negotiations at the UN level failed in 2017, cybersecurity experts have been calling for "coalitions of the willing" from G20 or G7 states to drive international norm-setting forward. Two-track formats, such as the Global Commission on the Stability of Cyberspace, predominate. However, strengthening attribution concerns not only states but also the private sector. In February 2017, Microsoft called for a "Digital Geneva Convention."[12] The most recent initiative, a "Charter of Trust"

---

9 "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," *United Nations General Assembly*, A/70/174, July 22, 2015, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

10 "China, Russia Sign Joint Statement on Strengthening Global Strategic Stability," *Xinhuanet*, June 26, 2016, http://www.xinhuanet.com/english/2016-06/26/c_135466187.htm.

11 Adam Greer and Nathan Montierth, "How Are US-China Cyber Relations Progressing?," *The Diplomat*, November 01, 2017, https://thediplomat.com/2017/11/how-are-us-china-cyber-relations-progressing/.

12 Brad Smith, "The need for a Digital Geneva Convention," *Microsoft*, February 14, 2014, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

launched by Siemens at the Munich Security Conference in February 2018,[13] sets the same course. Finally, the World Economic Forum aims to create a Global Center for Cybersecurity to combat cybercrime and thus also improve cooperation between the private sector and state authorities, the so-called public-private partnerships.

The EU's Cyber Foreign and Cybersecurity Policy

Cybersecurity is an issue not only for states but for the EU as well. It extends beyond the resilience of networks, the digital single market, or the prosecution of cyber criminals, and also concerns the EU's CFSP and the EU's Common Security and Defense Policy (CSDP) (see Table 1 below). A range of actors already tackle the EU's cyber foreign and cybersecurity policy within its Integrated Political Crises Response (IPCR) and most significantly in the EU Agency for Network and Information Security (ENISA); the European Cybercrime Center (EC3) at Europol; the EU Intelligence and Situation Center (INTCEN); the Intelligence Directorate of the EU Military Staff (EUMS INT) and its situation room (EU SITROOM); the EU INTCEN unit for analyzing hybrid threats, known as the Hybrid Fusion Cell; the Computer Emergency Response Team for EU institutions and agencies (CERT-EU); and the European Commission's Emergency Response Coordination Center (ERCC). New structures and mechanisms created under the Network and Information Security (NIS) directive, such as the member states' network of IT emergency teams (CSIRTs), must also be acknowledged.

At the EU level, the Horizontal Working Party on Cyber Issues was created in 2015 to coordinate the political aspects of cyberspace within the council. It participates in both legislative and non-legislative activities. Furthermore, EU member states decided in February 2015 to strengthen cyber diplomacy at the EU level in the EEAS. This was confirmed in November 2016 by the implementation plan on security and defense.[14] Important bodies that coordinate the strategic upstream analysis for the CFSP are the cyber diplomacy team in the EEAS as well as the EU INTCEN for civilian situational awareness and

13 "Charter of Trust Time for Action: Building a Consensus for Cybersecurity," *Siemens*, May 17, 2018, https://www.siemens.com/innovation/en/home/pictures-of-the-future/digitalization-and-software/cybersecurity-charter-of-trust.html.

14 "Implementation Plan on Security and Defence, Factsheet," *European External Action Service*, 2016, https://eeas.europa.eu/headquarters/headquarters-homepage/34215/implementation-plan-security-and-defence-factsheet_en.

Table 1. Cyber Security in the European Union: Areas of Responsibility

	Freedom, security, justice	Single market	CSDP: Cyber defense	CFSP: Cyber diplomacy
EU	Europol (EC3) Eurojust EU-LISA	ENISA CSIRT network CERT-EU	EDA GSA	EEAS SIAC (EU INTCEN, EUMS INT) EU SITROOM EU Hybrid Fusion Cell ERCC
National	Executive and data-protection authorities	Authorities in charge of NIS, National CSIRTs	Defense, military, and security agencies	Foreign ministries

Abbreviations: *EDA*: European Defense Agency; *EEAS*: European External Action Service; *EU-LISA*: European Agency for the Operational Management of Large-scale IT Systems in the Area of Freedom, Security and Justice; *GSA*: European Global Navigation Satellite Systems Agency; *SIAC*: Single Intelligence Analysis Capacity.

the EUMS INT for the military. To deter and reconstruct cyberattacks and to identify the perpetrators, forensic computer scientists depend on numerous sources in different states and companies on all political levels. To establish coordination in this area, the European Union can rely on well-established cooperation between ministries and security agencies. Special rules apply for the fight against terrorism. However, an EU-coordinated policy that brings together binding exchanges of information with surveillance and the use of that shared information has not yet been enshrined as an EU competence in the treaties but is subject for reconsideration. The protection of the digital internal market justifies an increasing competence of the European Commission in this regard. Julian King, the commissioner for the Security Union is herewith in charge and has launched a far-reaching legislative package for strengthening the resilience within the internal market.

The European Union's Joint Communication on "Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU" of September 2017 offers starting points for cooperation, which build both confidence and security and are based on the four pillars of EU cyber security.[15] The Horizontal

15 "Resilience, Deterrence and Defence: Building Strong Cybersecurity in Europe," *European Commission*, 2017, https://ec.europa.eu/digital-single-market/en/news/resilience-deterrence-and-defence-building-strong-cybersecurity-europe.

Working Party on Cyber Issues, chaired by the rotating presidency, and the Political and Security Committee (PSC) are responsible for appropriate implementation measures. Legally, EU member states are free to launch initiatives.

The four pillars of EU cyber security are as follows:

First pillar: The provisions of the Directive on Attacks against Information Systems of 2013,[16] including its penalties, are applicable in the case of criminal actors without significant ties to a state sponsor. To counter the growing threat of cross-border cybercrime, new instruments are planned that can be used to prosecute perpetrators more effectively. An "e-evidence" directive is currently being negotiated to facilitate cross-border access to electronic evidence.[17] Also under discussion is a directive on fighting fraud and forgery in cashless media, such as bitcoin. This aims to improve cooperation between criminal justice authorities.

Second pillar: ENISA is being upgraded, having increased its staff from around 80 to 125 and its annual budget from 11 to 23 million euros. The agency is expected to organize yearly pan-European cybersecurity exercises and steer cooperation between the member states' Computer Security Incident Response Teams (CSIRTs). Previously, these exercises were occasionally extended to allied non-member states. ENISA is primarily meant to accompany the establishment and implementation of an EU-wide certification framework. The objective is to make IT products and services more secure through market incentives and to enable users to make informed purchasing decisions. Divergent certification systems will be harmonized to strengthen the digital single market for trustworthy products. These measures are based on the NIS directive,[18] which will come into force in

16 "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," *European Parliament*, 2005/222/JHA, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF.

17 "E-evidence – Cross-Border Access to Electronic Evidence," *European Commission*, https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en.

18 "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union," *European Parliament*, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

May 2018; it serves as a benchmark for attaining similar improvements in the OSCE as well.

Third pillar: In December 2017, the twenty-five EU defense ministers established Permanent Structured Cooperation (PESCO).[19] In November 2018, seven of thirty-four projects are explicitly dedicated to Europe's cybersecurity. According to reports, others concern the standardization of soldier systems, meaning electronic equipment, linguistic and data communications, and software. Greece plans to develop a European IT emergency team; Lithuania wants to be in charge of establishing a European cyber defense. The idea is to create a "cyber Schengen area" to combat online criminality operating across all national borders. By late 2020, the European Investment Bank intends to invest more than six billion euros in developing so-called dual-use technologies for cyber security and civilian security.

Fourth pillar: The European Union is conducting bilateral cyber dialogues within its strategic partnership agreements with the United States, Canada, China, South Korea, and so forth. The European Union also proposes drawing up a strategy for international cooperation in cyberspace and conflict prevention, in line with the cybersecurity reform of September 2017. As a first step, it has updated the CFSP and CSDP's instruments as well as its directive on export controls for dual-use goods.

Joint EU Diplomatic Response to Malicious Cyber Activities

The increase in cyberattacks has forced international actors to consider how to respond appropriately. The Obama administration imposed unilateral sanctions for the first time in 2014 after a US subsidiary of the Sony Corporation fell victim to a devastating cyberattack, during which all company data were copied.[20] Two years later, Washington reacted similarly when the US administration's personnel data were siphoned during a large-scale cyberattack. Following the alleged Russian interference in the 2016 US presidential election campaign, the United States imposed sanctions in March 2018 on five companies and organizations as well as nineteen individuals,

19 "Permanent Structured Cooperation (PESCO) – Factsheet," *European External Action Service*, 2018, https://eeas.europa.eu/headquarters/headquarters-Homepage/34226/permanent-structured-cooperation-pesco-factsheet_en.

20 David E. Sanger and Michael S. Schmidt, "More Sanctions on North Korea After Sony Case," *New York Times*, January 2, 2015, https://www.nytimes.com/2015/01/03/us/in-response-to-sony-attack-us-levies-sanctions-on-10-north-koreans.html.

citing Russia's "malicious cyber activities."[21] The European Union had first discussed the necessity for joint cyber diplomacy in February 2015. In June 2017, it suggested establishing a Cyber Diplomacy Toolbox so as to provide a joint diplomatic response to malicious cyber activities.[22] Its main goal was to guarantee the responsiveness of its foreign and security policy below the threshold for armed conflict. This would complement its efforts under the NIS directive to push through minimum standards and reporting obligations as well as build resilient IT and communications systems in the digital single market. At the EU level, responding to attacks with cyber diplomacy above triggers the political measures contained in the CFSP, including restrictive measures.

In October 2017, the planned Cyber Diplomacy Toolbox was adopted under its new title of "Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities." Its purpose is to facilitate cooperation in containing immediate and long-term threats and to help deter culprits and potential attackers in the long term. Individual states apparently did not have sufficient reach to affect attackers' cost-benefit calculations; EU diplomacy, by contrast, offered a strategic added value due to its ability to impose sanctions or positive incentives. The European Union has committed to international principles upholding due diligence in cyberspace and intends to strengthen cyber diplomacy in exchanges with third parties with the aim of combating cyberattacks. The UN's Group of Governmental Experts (GGE) incorporated the principle of upholding due diligence in its final report of June 2015.[23] According to this report, states should ascertain that their sovereign territory and the computer systems and infrastructure located there or otherwise under their control are not misused for attacks on the infrastructure of other states.

---

21 "Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks," *US Department of the Treasury*, March 15, 2018, https://home.treasury.gov/news/press-releases/sm0312.

22 "Draft Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (Cyber Diplomacy Toolbox) 9916/17," *European Council*, June 7, 2017, http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf.

23 "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," *United Nations*, July 22, 2015, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

Five Different Measures

In its cyber diplomacy, the European Union relies on the CFSP toolbox. Its measures can be divided into preventative, cooperative, stabilizing, and restrictive, as well as member states' lawful responses for self-defense. Political measures are determined by the EU Council with the assistance of the European External Action Service. In grave instances, malicious cyber activities could amount to punitive measures and the use of force or an armed attack in accordance with international law and the Charter of the United Nations. In this case, member states take a sovereign decision to exercise individual or collective self-defense as recognized in Article 51 of the UN Charter and in accordance with international and humanitarian law.

Prevention: Within the its political dialogues with third states, the European Union has developed cyber dialogues that aim to influence the behavior and attitude of its dialogue partners. The European Union also supports CBMs such as those developed by the OSCE. Dialogues with regional organizations, such as the African Union or ASEAN (Association of Southeast Asian Nations) are particularly important. The European Union and the respective regional body can define how to build up the region's capacities for using cyberspace (known as "cyber capacity building") in association, partnership, or cooperation agreements, or even through the Instrument contributing to Stability and Peace (IcSP).

Cooperation: To facilitate an ongoing incident, an EU delegation in a host country can transmit a diplomatic note (démarche) to that country's government. This requires an instruction from the high representative of the Union for Foreign Affairs and Security Policy. In a conflict situation, the delegation head can deliver a proposal to conduct comprehensive talks or merely convey key messages. Démarches can also be formulated and delivered together with third states. Where the EU delegation head has been recalled due to conflict, this type of cooperative solution is no longer possible.

Stability: These measures have a signaling function by serving as a strategic communication that the potential aggressor should refrain from engaging in malicious cyber activities The European Council can set out an EU act or position but only unanimously. It can also pass a resolution to implement such an act. In that case, qualified-majority voting applies, except for acts of implementation concerning the military or defense (art. 31, para. 2 Treaty on European Union [TEU]). The high representative of the Union for Foreign

Affairs and Security Policy can also make a declaration "in the name of the European Union." However, this has to be agreed beforehand with all EU states and is usually employed if there is no need for an immediate response, if the EU first has to work out its position vis-à-vis a new situation, or if it has modified an established position. However, the high representative can also make a declaration under his/her own responsibility if a quick reaction is required, but it is not possible to seek agreement from the EU 27.

Sanctions: The European Union can impose restrictive measures (sanctions) if it intends to push through political objectives following serious cyberattacks. These measures tend to target government officials of third states but also state companies or other legal or natural persons. The council has to vote unanimously for sanctions and they must conform to the CFSP's objectives under Article 24 of the Treaty of the European Union. Sanctions can be divided into two main categories: Those decided autonomously by the EU and those that the EU is obliged to impose following a resolution by the UN Security Council. Under EU law, sanctions must be targeted. For instance, specific persons or companies may be put on a sanctions list in order to block their bank accounts as long as minimum rule-of-law standards are met. So-called prerequisites for legality have been drawn up for such cases, which stipulate, for example, that those targeted have to be informed of the reasons for being listed and be given the opportunity to file a complaint.

Possible EU support to member states' lawful responses: The Lisbon Treaty introduced the solidarity and mutual-assistance clauses, which can be invoked after severe cyberattacks. The solidarity clause (Article 222 of the Treaty of the Functioning of the European Union [TFEU]) stipulates that EU member states provide mutual support if one or several of them are victims of terror attacks, natural disasters, or man-made disasters (including serious cyber incidents). Its implementation procedure was defined by European Council decision in July 2014. The mutual-assistance clause contained in Article 42, para 7 of the TEU roughly corresponds to Article 5 of the NATO Treaty, although the latter takes precedence for NATO members. The mutual-assistance clause was invoked for the first time in November 2015 by France following the Paris terror attacks. Under the Joint EU Diplomatic Response to Malicious Cyber Activities of October 2017, responses that are compliant with international law do not require unequivocal attribution of cyberattacks to specific origins or perpetrators. This accords with the

interpretations of international law experts enshrined in the Tallinn 2 Manual on how international law applies to cyberspace.

Export Controls

The European Union intends to promote its cyber diplomacy and aspiration to due diligence by more strictly controlling the export of dual-use goods. The dual-use directive of May 2009 regulates the member states' joint licensing requirements for the export, procurement, and transit of such goods. In mid-December 2017, the European Commission published a new version of the directive's annexes I, IIa to IIg and IV.[24] The update mainly concerned new controls for certain goods, such as IT hardware. Goods are categorized as subject to control (Annex I) based on (1) the stipulations of international treaties and obligations, especially UN Security Council Resolution 1540, the Chemical Weapons Convention and the Biological Weapons Convention, and (2) the control lists of international multilateral export regimes, above all the Wassenaar Arrangement, the Nuclear Suppliers Group, the Australia Group, and the Missile Technology Control Regime (MTCR). These lists in particular are constantly modified. Not only is the export of specific goods to states under sanction subject to tighter controls, but in many cases separate approval also has to be obtained for exporting dual-use goods. Non-compliance can result in stiff penalties or fines.

Due Diligence, Step-by-Step

The European Union's unanimity requirement makes positioning it as a force for peace difficult. Its member states exhibit not only great strategic ambivalence, for instance in their policy toward Russia, but they also lack coherence in their actions in foreign affairs. The EU's aspiration to act as a force for peace is manifested by member states seeking to strengthen the due-diligence principle via the CFSP's political instruments. Due diligence is a well-accepted principle in international law, based on the idea that the EU not only has to guarantee that rules are upheld in its own jurisdiction but also needs to bear responsibility for the consequences of its actions beyond

24 "Commission Delegated Regulation (EU) 2017/2268 of 26 September 2017 amending Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items," *Official Journal of the European Union* 60, December 15, 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2017:334:FULL&from=EN.

its borders, for instance through a more strict export policy. Ever more frequently, EU decisions reach beyond its jurisdiction. It is the European Union's role—and its role alone—to create coherence in this area. Where protecting cyberspace is concerned, member states should not limit themselves to avoiding irresponsible solo decisions. They must also undertake everything that reasonably could be expected from them to contribute, along with other states, to an "open, global, free, peaceful, and secure cyberspace."

There is debate over how far EU governments should prepare to take technical countermeasures or even carry out hackbacks, as is currently being considered in the case of Russia. This would be the highest level of escalation under the mutual-assistance clause when a member state chooses to invoke self-defense as recognized in Article 51 of the UN Charter and in accordance with international law, including humanitarian law. The final step of crisis management would then consist of stopping an ongoing attack through active defense. *Ultima ratio* would be a so-called hackback, meaning the targeted elimination of the server from which an attack has been launched. This only complies with the principle of due diligence if the ongoing attack has serious consequences that threaten a state's survival and if all other means have been exhausted. The legal framework and the distribution of competences this requires have not been defined, not even at the national level.

The EU's most important and lastingly effective tools in this context are prevention and detection. Prevention encompasses the measures contained in the NIS directive, such as the introduction of minimum standards and reporting requirements for operators of critical infrastructure. Telecommunications providers are allowed to analyze data traffic in case of disturbances and, if necessary, block the culprits they identify.

Detection is the elucidation and attribution of attacks. Here, political evaluation is decisive. It has to take into account the overall picture of cyber incidents to anticipate militarily relevant hybrid threats. Where professional attacks are concerned, cyber diplomacy between likeminded states is necessary for security agencies to share analyses of code fragments and of the way the attack unfolded. Such analyses often make it possible to draw conclusions about hacker groups and their origins. The CSIRT network and its technical competence is meant to provide a similar exchange for Critical Infrastructure Protection. Cyber diplomacy also requires authorities and businesses to exchange information. Public and private CERT groups

and alliances in industry are indispensable for pooling expert knowledge in cyber diplomacy as well.

Cyber diplomacy is an important component of national cyber security, but it also has to integrate the European and even global dimension. Investigations based exclusively on national information are insufficient. With its Joint EU Diplomatic Response Framework of 2017, the EU has opted for a non-military cybersecurity policy. This helps resist the temptation to respond immediately to threats in cyberspace. Instead, the European Union privileges political measures as part of the CFSP, so as to make its mark as a force for peace. This approach should be understood as a clear political signal by its partners and competitors worldwide.

Global Changes in the Proliferation of Armed UAVs: Risks, Challenges, and Opportunities Facing Israel

Liran Antebi

For a number of decades, Israel has been among the leaders in the manufacture, export, and operation of unmanned aerial vehicles (UAVs). This position has given Israel a security advantage and has affected its relations with various countries. In recent years, significant changes have occurred in this sphere, as new manufacturers and exporters, such as China, Iran, and Russia, have appeared, while the United States has changed its export policy. Growing use is being made of civilian technologies and tools, such as drones converted to military use by both countries and terrorist organizations. These changes potentially could have a substantial effect on Israel, both in terms of security and trade. This article reviews the developments that have taken place in the worldwide proliferation of UAVs and recommends a suitable policy for the State of Israel in order to address these changes, including expanding intelligence monitoring of proliferation of UAV systems and components, investing in cyber and electronic warfare systems to counter UAVs, increasing transparency in manufacture and development, and supporting civilian development aimed at entering new markets.

Keywords: UAVs, unmanned systems, drones, military technology

Dr. Liran Antebi is a research fellow at the Institute for National Security Studies and a lecturer at Tel Aviv University and Ben-Gurion University of the Negev. The author wishes to thank Ms. Matan Yanko-Avikasis, an MA student in diplomacy at Tel Aviv University and an intern at the Institute for National Security Studies.

Cyber, Intelligence, and Security | Volume 2 | No. 3 | December 2018

Introduction

Israel is a major player in the global UAV industry. This is reflected in the development and manufacturing of advanced systems, the accumulation of varied operational experience, and exports of unmanned aircraft. For seven years (2005–2013), Israel was the world's leading exporter in this sphere, despite being a fairly small country.

In recent years, the proliferation of UAVs, including armed UAVs, has changed substantially. This development resulted from the entry of new manufacturers and exporters into the market; a change in the policy of established exporters; and technological developments facilitating the use of various civilian components and products that have been adapted and converted to defense needs. These changes can potentially affect Israel both in terms of security and trade.

This article begins by describing Israel's dominance in the field of UAVs in the past decades and then portrays the changes that have occurred in the proliferation of UAVs in the last decade, including a discussion of the shifting patterns in their use. The article also proposes ways of coping with these changes. In addition to preparing for the security threats posed by this new situation, a change of policy is also needed in the development and production of UAVs in order to maintain Israel's strength in this field.

Israel's Dominance in the Field of UAVS

Israel has been one of the dominant players in the field of UAVs for decades. Israel began using them for photography purposes as early as the 1960s and 1970s, and later for deception and intelligence gathering, notably in Operation Mole Cricket 19 (ARTZAV 19) at the beginning of the First Lebanon War in 1982. Some believe that the success of the UAV activity in this operation inspired continued development of UAVs in the United States in the 1980s and 1990s.[1]

Despite the impressive military operations that featured the early UAVs, Israel's main use of unmanned systems was for ISR as part of its asymmetric warfare, beginning with a series of operations in the early 2000s to the Second Lebanon War, and followed by operations against Hamas (Operation Cast Lead, Operation Pillar of Defense, and Operation Protective Edge) in the

1 Tamir Libel and Emily Boulter, "Unmanned Aerial Vehicles in the Israel Defense Forces," *RUSI Journal* 160, no. 2 (2015): 68–75.

Gaza Strip. Israel's use of UAVs reached a peak in 2006 when it became the first country in history to record more UAV flight hours than manned fighter jets flight hours during a war. Furthermore, it was the first case in military history in which UAVs were continuously used above the battlefield during an entire war.[2]

Israel's leading position and dominance in the field of UAVs is not confined to operational experience. Despite being a relatively small country, Israel was the leading global exporter of UAVs during 2005–2013, with exports totaling $4.62 billion.[3] According to various reports, Israel exported unmanned aerial vehicles to many countries in Europe, Asia, and Latin America,[4] and for many years, Israel also exported UAVs to the United States, which used them in the war in Iraq, among other things.[5] Currently, Israel manufactures and exports various types of unmanned aerial systems on a large scale, including tactical mini-UAVs operated by ground forces, such as Skylark by Elbit Systems;[6] multi-purpose medium-range tactical systems, such as Elbit Systems' Hermes 450, which has a flight range of hundreds of kilometers and is capable of carrying special payloads of approximately 200 kilograms;[7] and long-range UAVs, such as Heron, by the Israel Aerospace Industries' (IAI), which is capable of carrying a special payload of up to 470 kilograms.[8] According to foreign reports, some of the remotely operated Israeli UAVs have advanced attack capabilities.[9]

---

2 Isaac Ben-Israel, "The First Israel-Hizbollah Missile War (Summer 2006)," a position paper by the College of Policy and Government, Tel Aviv University, May 2007, p. 46.

3 Ora Coren, "Israel is the World's Largest Exporter of Drones," *The Marker*, May 19, 2013 [in Hebrew], https://www.themarker.com/news/macro/1.2023690.

4 Harriet Sherwood, "Israel is World's Largest Drone Exporter," *The Guardian*, May 20, 2013, https://www.theguardian.com/world/2013/may/20/israel-worlds-largest-drone-exporter.

5 Amnon Barzilai, "U.S. Army Wants to Buy More Israeli Hunter Drones," *Haaretz*, July 8, 2003, https://www.haaretz.com/1.5494046.

6 Skylark^{tm} I – LEX, Elbit Systems website, http://elbitsystems.com/products/uas/skylark-i-lex/.

7 Hermes^{tm} 450, Elbit Systems website, http://elbitsystems.com/products/uas/hermes-450/.

8 Heron, Israel Aerospace Industries website, http://www.iai.co.il/2013/18900-16382-en/BusinessAreas_UnmannedAirSystems_HeronFamily.aspx.

9 Ron Ben-Yishai, "Uncertainty about UAV Attacks Unnecessary," *Ynet News*, July 11, 2016 [in Hebrew], https://www.ynet.co.il/articles/0,7340,L-4826915,00.html.

In addition to these systems, which are flown and operated remotely, Israel also manufactures and exports UAVs in the loitering munitions category, some of which are autonomously operating fire-and-forget systems. These UAVs have technical capabilities that enable them to fly, remain airborne, track a target, and—if necessary—destroy it in a kamikaze mission with explosives they carry. This involves either minimal human intervention, or none at all. Among the prominent systems in this category are Harpy NG and Harop, manufactured by IAI.[10]

Exports of UAVs are one of Israel's important commercial sectors, which, at one point, accounted for about 10 percent of all its defense exports.[11] Beyond its economic importance, exports of UAVs have a major impact on Israel's relations with various countries, both diplomatically and in terms of defense cooperation. Prominent in this framework is Israel's UAV transaction with Russia (to which the United States made no objection), in exchange for which Israel expected Russia to refrain from selling S-300 missiles to Iran.[12]

While for many years, Israel was the leading UAV exporter, the United States also led in producing UAVS and invested considerable resources in manufacturing them in order to increase its own order of battle. In recent years, however, a process has begun in which American UAV manufacturers are seeking to sell such systems to various countries around the world. As a result, this development has intensified global competition, and, above all, competition with Israel. At the same time, additional changes are taking place in the proliferation of military UAVs throughout the world, as described below. These changes are also likely to affect Israel.

A Change in the Proliferation of Military UAVs

The global UAV market has grown substantially from year to year. The market, which was estimated at $5.93 billion in 2015, is projected to reach $22.15 billion in 2022. Although the military sector of the market will

10 Harpy NG, Israel Aerospace Industries Website, http://www.iai.co.il/2013/36694-16153-en/Business_Areas_Land.aspx.

11 Coren, "Israel is the World's Largest Exporter of Drones."

12 Anshel Pfeffer, "Israel to Sell UAVs in Exchange for Canceling Deal with Iran," *Haaretz,* June 25, 2009 [in Hebrew], https://www.haaretz.co.il/news/politics/1.1267820.

grow, most of the market growth will be in the civilian sector.[13] Despite the global changes, Israel and the United States are still the two leaders in manufacturing and exporting military UAVs. Technological innovations, together with the effects of globalization and the absence of regulation, have caused significant changes in this field and have facilitated the appearance of new players in the UAV market.[14] The new players are offering their wares in new markets, including countries to which formerly no party was willing to sell systems of this type.

This development has led to significant changes in the proliferation of UAVs in general and armed UAVs in particular, as well as in the patterns of their use. This matches the forecast made a number of years ago by the RAND Corporation, which forecasted that within a decade, every country would be able to purchase and employ armed UAVs.[15] Based on the RAND Corporation's study and the changes that have taken place since it was published, it can be argued that the most significant change in the UAV sector today is taking place in the armed UAV sub-sector.

China is one of the important players that has entered the armed UAV export market in the past decade and has caused fundamental changes to it. According to a 2015 report by the US Department of Defense, China plans to manufacture 42,000 various types of UAVs by 2023,[16] while more recent reports state that China continues to invest resources in this field in order to

13 Christopher Diamond, "Global Drone Market Expected to Surpass $22B by 2022," *Defense News*, May 3, 2017, https://www.defensenews.com/air/2017/05/03/global-drone-market-expected-to-surpass-22b-by-2022/.

14 Liran Antebi, "Changing Trends in Unmanned Aerial Vehicles: New Challenges for States, Armies, and Security Industries," *Military and Strategic Affairs* 6, no. 2 (August 2014), http://www.inss.org.il/publication/changing-trends-in-unmanned-aerial-vehicles-new-challenges-for-states-armies-and-security-industries/.

15 Lynn E. Davis, Michael J. McNerney, James S. Chow, Thomas Hamilton, Sarah Harting, and Daniel Byman, *Armed and Dangerous? UAVs and U.S. Security* (Santa Monica: RAND Corporation, 2014), https://www.rand.org/pubs/research_reports/RR449.html; Patrick Tucker, "Every Country Will Have Armed Drones Within 10 Years," *Defense One*, May 6, 2014, https://www.defenseone.com/technology/2014/05/every-country-will-have-armed-drones-within-ten-years/83878/.

16 Zachary Keck, "China Is Building 42,000 Military Drones: Should America Worry?," *National Interest*, May 10, 2015, https://nationalinterest.org/blog/the-buzz/china-building-42000-military-drones-should-america-worry-12856.

carry out its plan.[17] Chinese Cai Hong (CH) Rainbow UAVs, manufactured by China Aerospace Science and Technology Corporation (CASC),[18] have been widely distributed throughout the world over a few years time. Notable among this series are the CH-3, the most common model, and the CH-4. Both have offensive capabilities but differ in size, payload capacity, and duration of flight. The manufacturer claims that the CH-5, the newest UAV of this series, can carry payloads and weapons weighing up to 1,000 kilograms, with sixty hours endurance, and has a maximum flight range of 6,500 kilometers.[19] These figures are an attempt to compete with advanced UAVs made by countries that have a great deal of experience in this field.

Simultaneously with its rapid technological and production development, China practices a very permissive and liberal export policy, in contrast to the conservative policy of the United States and Israel. For one, China has not signed agreements such as the Missile Technology Control Regime (MTCR), which restricts UAV exports. The Chinese also offer a variety of their UAVs at significantly lower prices than the Americans do, which makes China an attractive exporter. For example, a Chinese CH-5 UAV costs almost half the price of an American MQ-1 Predator UAV.[20] As a result, Pakistan, Iraq, and Nigeria have already conducted attacks using armed UAVs supplied to them by China or manufactured with its cooperation. As of 2018, China has approved UAV exports to ten countries, including Jordan, Saudi Arabia, and the United Arab Emirates.[21] This Chinese policy affects Israel both in terms of security and trade.

Another player causing change in the global UAV market is Iran. In recent years, Iran has been manufacturing various types of UAVs, displayed

17 US Department of Defense, "Annual Report to Congress, Military and Security Developments Involving the People's Republic of China 2018," May 16, 2018, pp. 23, 33–34, 63–64, 83, https://media.defense.gov/2018/Aug/16/2001955282/-1/-1/1/2018-CHINA-MILITARY-POWER-REPORT.PDF.

18 China Aerospace Science and Technology Corporation (CASC), http://english.spacechina.com/n16421/index.html.

19 Zhao Lei, "Unmanned Combat Drone to be Exported," *China Daily*, January 11, 2016, http://www.chinadaily.com.cn/china/2016-11/01/content_27233618.htm.

20 Ben Brimelow, "Chinese Drones May Soon Swarm the Market – and That Could Be Very Bad for the US," *Business Insider*, November 16, 2017, https://www.businessinsider.com/chinese-drones-swarm-market-2017-11.

21 "World of Drones," *New America*, https://www.newamerica.org/in-depth/world-of-drones/1-introduction-how-we-became-world-drones/.

publicly on different occasions, although some of the models that Iran has displayed at exhibitions or in military parades do not have any operational capability. Up until recent years, it appeared that the Iranian-made UAVs were for use by its allies and protectorates, such as Hezbollah.[22] In the past two years, however, Iran apparently also began supplying UAVs to Syria, a failed country engaged in a civil war for over five years. This new development is a game changer for Israel.

One of the main systems used by Iran and its allies is the Shahed 129, which, among other things, was used to attack the rebels in Syria.[23] Iran has been offering a UAV called Hamaseh since 2017, which UAV scholars say is reminiscent of IAI's Heron TP (although its dimensions are smaller).[24] According to the Iranian reports, this UAV is capable of carrying advanced munitions and sensors, with endurance of eleven hours, and has a maximum flight range of 200 kilometers. The Iranians also claim that this UAV has stealth capabilities, although its external form and the way its munitions are mounted indicate otherwise.[25] As Iran does not have any military satellites, its ability to operate UAVs is therefore limited, because the transmission ranges of its UAVs are limited to relatively short distances. In other cases, the intelligence information that they gather can be transmitted only after they land.[26]

Together with the changes in proliferation of UAVs resulting from the new players entering the market, the United States—an established manufacturer of UAVs—is also likely to begin changing its policy on UAV exports, especially

22 Roi Kais, "Hezbollah Has Fleet of 200 Iranian-made UAVs," *Ynet,* November 25, 2013, https://www.ynetnews.com/articles/0,7340,L-4457653,00.html.

23 Jeremy Binnie, "Analysis: Syrian Rebel Video Corroborates Iranian UAV Strike Claims," *Jane's 360*, February 12, 2016, https://www.janes.com/article/57968/analysis-syrian-rebel-video-corroborates-iranian-uav-strike-claims.

24 Stephan Trimble, "Iran Puts Hamaseh UAV on Export Market," *FlightGlobal*, July 18, 2017, https://www.flightglobal.com/news/articles/iran-puts-hamaseh-uav-on-export-market-439414/.

25 Kelsey D. Atherton, "Iran Unveils Absurd New Stealth Drone," *Popular Science*, May 13, 2013, https://www.popsci.com/technology/article/2013-05/iran-unveils-new-stealth-drone-isnt.

26 Yaniv Kubovich, "Iran's Army of Drones, Target of Syria Strike: Rising Force or Limited Threat?," *Haaretz*, April 12, 2018, https://www.haaretz.com/middle-east-news/iran/.premium.MAGAZINE-iran-s-drones-targeted-in-syria-rising-force-or-limited-threat-1.5992631.

armed UAVs, and it will follow the example of those countries affecting the changes in the worldwide proliferation of UAVs. It was reported that President Trump, in contrast to his predecessor, was considering to change US export policy on unmanned systems. In the framework of the new policy, the barriers preventing the sale of small UAVs will reportedly be lowered for those with strike-enabling technology that have ranges and weapons payload capacities inferior to those of the veteran MQ-1 Predator UAV[27] or the MQ-9A Reaper, the more advanced model. The demand to lower the barriers to the sale of UAVs comes from the American defense industries, which seek to expand their circle of customers. Others in the United States oppose this change in policy, because, in part, they claim that increased sales of offensive UAVS are liable to give weapons to governments that take irresponsible actions against their neighbors and also against their own populations.[28]

Another country that seeks to become a more significant player in the field of the UAVs is Russia. Compared to its military power and the role its military exports play in its strategic relations with many countries, Russia is relatively backward in the field. Nonetheless, Russia is generally regarded as one of the five leading countries in the UAV field,[29] likely because of its efforts to invest resources in a national UAV development program costing billions of dollars.[30] Russia is also pursuing cooperation in UAV production with various other countries with which it previously had such cooperation.[31] Russia is still technologically and industrially backward in this field, but its

27 Michael C. Horowitz and Joshua A. Schwartz, "A New U.S. Policy Makes it (Somewhat) Easier to Export Drones," *Washington Post*, April 20, 2018, https://www.washingtonpost.com/news/monkey-cage/wp/2018/04/20/a-new-u-s-policy-makes-it-somewhat-easier-to-export-drones/?utm_term=.2f0fe76beefb/.

28 Mike Stone and Matt Spetalnick, "Exclusive: Trump to Boost Exports of Lethal Drones to More U.S. Allies – Sources," *Reuters*, March 18, 2018, https://www.reuters.com/article/us-usa-arms-drones-exclusive/exclusive-trump-to-boost-exports-of-lethal-drones-to-more-u-s-allies-sources-idUSKBN1GW12D.

29 Robert Farley, "The Five Most Deadly Drone Powers in the World," *National Interest*, February 16, 2015, https://nationalinterest.org/print/feature/the-five-most-deadly-drone-powers-the-world-12255.

30 Jaroslaw Adamowski, "Russian Defense Ministry Unveils $9B UAV Program," *Defense News*, February 19, 2014.

31 Yaakov Lappin, "Report: Moscow Purchased 10 Israeli Drones," *Jerusalem Post*, September 8, 2015, https://www.jpost.com/Israel-News/Politics-And-Diplomacy/Report-Russia-purchased-ten-Israeli-drones-415575.

growing activity requires special attention, especially given that it supplies military equipment to recalcitrant countries like Syria.

Parallel to these changes and forming a prominent trend, many countries have become UAV manufacturers, usually for their own consumption. Even though most of the UAVs being manufactured are not offensive, the potential effect of this change on both defense and trade cannot be ignored. These relatively new manufacturers include India, Pakistan, South Africa, Venezuela, and Ukraine, but many more countries can be mentioned in this context.[32]

Given the global changes taking place in the field of UAVs, several initiatives aimed at limiting or changing the existing situation have been launched. A study by the United Nations Institute for Disarmament Research (UNIDIR) calls for greater transparency, monitoring, and legal liability for armed UAVs. The study, based on meetings with experts in different fields and from various countries, includes a series of recommendations, the most important of which is conducting an open and joint multilateral discussion for the purpose of setting standards and principles for the use of armed UAVs.[33] In addition, the United States launched an initiative in 2016, in which it drew up a document of principles for regulating UAV exports. Although forty countries have signed the document to date, France, Russia, China, and Brazil are among the important manufacturers who refused to sign the document, in addition to Israel, which is concerned that the document will restrict its global business activity in this sphere.[34]

The Change in the Patterns of Using Armed UAVs

The change in the proliferation of UAVs facilitates, among other things, a shift in the patterns of their use, especially in the use of offensive UAVs. The majority of the shift in the use of UAVs in recent years has occurred in the

32 Wim Zwijnenburg and Foeke Postma, "Unmanned Ambitions: Security Implications of Growing Proliferation in Emerging Military Drone Markets," (Utrecht: Pax for Peace, 2018), pp. 18–35, https://www.paxforpeace.nl/publications/all-publications/unmanned-ambitions.

33 UNIDR, "Increasing Transparency, Oversight and Accountability of Armed Unmanned Aerial Vehicles," (2017), http://www.unidir.org/files/publications/pdfs/increasing-transparency-oversight-and-accountability-of-armed-unmanned-aerial-vehicles-en-692.pdf.

34 Gili Cohen, "Israel Refuses to Sign US Document Regulating Attack Drones," *Haaretz,* October 23, 2016 [in Hebrew], https://www.haaretz.com/israel-news/.premium-israel-won-t-sign-u-s-document-regulating-attack-drones-1.5452346.

Middle East, a region rife with violent conflicts. One prominent example is in the case of the Iraqi army's struggle against the Islamic State (ISIS) terrorist organization. The Iraqi army, which had been dismantled and rebuilt by the United States following the Second Gulf War, almost collapsed again under severe attack by ISIS; however, the Iraqi army currently possesses armed Chinese-made UAVs that have strike capabilities using guided missiles. These systems enable it to join a growing number of armies around the globe making operational use of armed UAVs, which, until less than a decade ago, had been limited to only a few countries. The case of Iraq is particularly disturbing, given the instability prevailing in that country in general and in the Iraqi army in particular.

According to a study by the PAX organization, new UAV manufacturers, such as Iran, supplied UAVs—some of them armed—to various countries for their use. Iranian-made UAVs have been used in a number of regional conflicts and clashes, including in Turkey, the Persian Gulf, and Syria, as well as in Pakistan, where Iranian-made UAVs were used against the rebels in northwestern Pakistan.[35] The ability of these countries to buy and use UAVs is disturbing, especially given the nature of their regimes, their instability, and the terrorist threats associated with them.

Another case in which offensive UAVs were used in the Middle Eastern theater is the Iranian UAV that Syria launched at Israel in February 2018. This UAV, which various sources assert is a copy of a US stealth UAV, having the capacity to carry precise missiles, was intercepted by Israel.[36] According to an inquiry conducted and published by the Israel Defense Forces, the UAV carried explosives, making its launch the first case in which Iran tried to directly attack Israeli territory.[37]

Beyond the use of the UAVs manufactured by the military industries of various countries, improvised armed weapons and converted civilian devices are now also being employed. Even though these devices were not produced

35 Zwijnenburg and Postma, "Unmanned Ambitions," p. 11.

36 Morris Loveday, "The Drone Shot Down by Israel was an Iranian Copy of a U.S. Craft, Israel Says," *Washington Post*, February 11, 2018, https://www.washingtonpost.com/world/israel-confirms-downed-jet-was-hit-by-syrian-antiaircraft-fire/2018/02/11/bd42a0b2-0f13-11e8-8ea1-c1d91fcec3fe_story.html?utm_term=.8ab82fb83acf.

37 Yoav Zitun and Ron Ben-Yishai, "The Explosive UAV: First Iranian Attempt to Attack Israel Directly," *Ynet* April 14, 2018 [in Hebrew], https://www.ynet.co.il/articles/0,7340,L-5229485,00.html.

for military purposes and are often small and have short ranges and little accuracy, they can still pose a significant security threat.[38] One prominent case in this context occurred in December 2017, when Khmeimim, a Russia air force base in the Latakia district, and Tartus, a logistics center, both in Syria, were attacked by a group of thirteen UAVs, causing substantial destruction to Russian army equipment: bombers, warplanes, cargo planes, and ammunition stores. The technology used by the attackers in their improvised devices, including GPS systems used for the precise attack, led Russian sources to claim that a developed country was behind the attack;[39] however, no concrete evidence of this allegation was found. Some scholars assert that sub-state organizations are also now capable of producing weapons like those used in the attack, using components that can be purchased commercially or self-produced. A few days after the first attack on Russian targets in Syria, known as the Novy God attack, the Russian army successfully thwarted another attempted attack against the Khmeimim base using armed UAVs.[40] Since then there have been additional attacks against the base, with the Russian air defense systems successfully intercepting the attack UAVs.[41]

The significance of these attacks is that UAV technology is now widely distributed, and the main threat to Israel comes not only from countries buying Iranian or Chinese attack UAVs but also from any group capable of assembling advanced attack devices from commercially available components. State intelligence organizations find it difficult to track such groups. This new threat is growing and becoming stronger as a result of the expanding proliferation of various types of advanced technologies. This creates an off-the-shelf supply of devices that can be used for deadly purposes without great difficulty. In this manner, various technologies have become dual use (civilian and military), even though they are not classified as such and

38 "Home-Made Drones Now Threaten Conventional Armed Forces," *Economist*, February 8, 2018, https://www.economist.com/science-and-technology/2018/02/08/home-made-drones-now-threaten-conventional-armed-forces.

39 Dave Majumdar, "Russia Came Under Attack by a 'Swarm' in Syria, Says Report," *National Interest*, January 8, 2018, https://nationalinterest.org/blog/the-buzz/russia-came-under-attack-by-swarm-syria-says-report-23987.

40 News agencies, "Russian Base in Syria Again Under Attack: 'Armed UAV Attack Thwarted'," *Walla News,* January 7, 2018, https://news.walla.co.il/item/3125331.

41 Dmitry Kozlov and Sergei Grits, "Russia Says Drone Attacks on its Syria Base Have Increased," *Times of Israel*, August 17, 2018, https://www.timesofisrael.com/russia-says-drone-attacks-on-its-syria-base-have-increased/.

are consequently not restricted by regulation or legislation that limits their distribution and prevents their use for military purposes. This constitutes a substantial threat to Israel, because the terrorist organizations that pose the threat rely on these technologies more than regular armies do.

The UAV attacks in Syria once again also highlight the threat of drones, which many countries are not prepared to face—neither in their deployment of air defense systems around bases and strategic assets, nor in electronic warfare or cyber capabilities for jamming or gaining control over hostile remote-controlled devices. The damage caused by improvised devices like the one used in the attacks against Khmeimim, or by an armed drone attack, does not have a strategic effect on a country or a military system in most cases, but they are liable to cause severe cognitive damage.

Possible Effects on Israel

The changes taking place in the field of UAVs affect the entire international arena. Armed UAVs have provided various groups greater capability, more than in the past, of carrying out aerial attacks without taking responsibility for them, while maintaining secrecy about the source of the attack. The ability to carry out ISR missions has also shifted significantly as a result of the change in risk management by commanders or politicians, due to the fact that these aircraft have no human operator on board. The growing competition in the UAV market is an additional factor that substantially affects other countries, especially those that were formerly leading manufacturers and exporters in this area.

The effect of these changes on Israel is greater than in other countries in both the defense and trade sectors. This is due to Israel's standing as a leading exporter of unmanned aerial systems, the effect of the proliferation of UAVs on strategic questions of concern to Israel, and the range of ongoing security threats against it from both neighboring countries and terrorist organizations operating both inside and outside Israel's borders. The changes in the UAV industry and their principle effects on Israel are discussed below.

Security Threats

The wide range of UAV manufacturers and exporters, including offensive UAVs, changes the nature of the potential users of these systems. The fact that countries that previously were unable to purchase UAVs (because of both the

cost and those countries' strategic relations) are now able to purchase them from China and use them is liable to pose a challenge to Israel in the near or medium-term future. The risk posed by the possibility of these systems moving from those countries into the hands of non-state groups should also be taken into account. The relevant countries in this context include Iraq, Jordan, Pakistan, and Iran, in addition to Hezbollah, which is equipped with Iranian systems.

It should be noted that this change comes in addition to other transformations in the Middle East, including the unstable situation in Syria over the past decade and the Russian and Iranian presence, which both affect Israel and create threats that it must face. To this should be added the aerial threat resulting from the use of drones and improvised weapons, plus the fact that various players are able to obtain significant aerial capabilities through commercially available off-the-shelf components. These capabilities include attack UAVs and improvised precise aircraft for use in suicide missions.

Commercial Challenges

The commercial challenges to Israel resulting from the proliferation of UAVs is a difficult one. Israel needs defense exports, of which UAVs constitute an important share, in order to advance large-scale activity by Israel's defense industries, since the Israeli market is too small to sustain those industries by itself. In addition, Israel's UAV exports are affected by global changes in the proliferation of unmanned aircraft, especially the Chinese UAV exports, which constitute significant commercial competition.[42] In contrast to the United States, however, which also suffers from Chinese competition, Israel is more exposed to international criticism for its use of UAVs, which is also liable to affect its manufacturing and export capacities.[43] Furthermore, in contrast to the United States, which can respond to competition from China and Israel by expanding its UAV exports to countries like Saudi Arabia,[44]

42 "Israeli UAV Manufacturers Fear Chinese Threat," *The Marker*, February 10, 2018 [in Hebrew], https://www.themarker.com/wallstreet/1.5806899.

43 Damien Gayle, "Charges Dropped over Protest at Israeli Military Drones Factory in UK," *The Guardian*, November 23, 2017, https://www.theguardian.com/world/2017/nov/23/charges-dropped-protest-israeli-military-drones-factory-uk-uav-engines.

44 Dan Arkin, "US to Supply Medium-Range Armed UAVs to Saudi Arabia, South Korea, and Japan," *Israel Defense*, March 26, 2018 [in Hebrew], http://www.israeldefense.com/he/node/33573.

Israel's export market is more limited, since it faces more difficulty than others in exporting UAVs to countries with which it has no official diplomatic ties.

Israel's exports, particularly the UAVs, are also affected by the defense export agreements. One prominent agreement is the Missile Technology Control Regime,[45] the supervisory regime for missile technologies, in which the member countries coordinate their policies of supervising exports in this sector. Since 1991, Israel has acted in accordance with this agreement and has applied it in countries to which it exports UAVs.[46] At the same time, as with other international agreements, Israel finds it difficult to have any influence on the occasional revisions made to the agreement, which have a greater commercial effect on it than on the United States as well as on countries that did not sign the agreement or do not comply with its provisions.

Both the defense and commercial challenges require Israel to revise its policy on UAVs in order to be suitably prepared for the risks of hostile operation of UAVs by Israel's enemies and to preserve its ability to export unmanned aircraft to various countries and to enjoy the economic and diplomatic benefits that it confers.

Recommendations for Israel

Given the changes described above, Israel must consider hostile operation of UAVs, drones, and improvised weapons as possible aerial threats by the countries that are its enemies. This has already occurred when UAVS were launched by Hezbollah in Lebanon toward Israel and from Syria, operated by Iran. Israel must also prepare to intercept and respond even in cases when weapons are used against it without any group taking responsibility for their launching. In addition, Israel should be aware of the risks involved in the proliferation of UAVs and should prepare technologically and operationally to address the small and medium-sized risks from unmanned aircraft that are likely to be utilized in a group or in a barrage.

Israel should devote intelligence efforts to tracking the worldwide proliferation of UAVs, including armed UAVs made by China, Iran, and other countries in the Middle East arena. In addition, it should monitor off-the-shelf products and components, as well as dual-use technologies likely

45 The Missile Technology Control Regime website: http://mtcr.info/.

46 The website of the Israeli Defense Export Controls Agency, http://www.exportctrl.mod.gov.il/Hakika/Pages/MTCR.aspx.

to help produce improvised unmanned aircraft. A thorough understanding of the global UAV map, combined with monitoring exports and the transfer of weapons between countries and between sub-state organizations, is an important element in preparing to defend Israel's skies and its forces in routine and war times.

Simultaneously, Israel should invest in developing cyber and electronic warfare systems, while adapting its air defense systems to threats from UAVs. The aim is to create cheaper responses than missile interception through remote jamming or disabling of hostile UAVs, for example. Israel also needs effective means for dealing with the multiplicity of large-scale threats, including groups and swarms of UAVs and drones.

Israel should assume that this trend will continue to mount and affect the international arena. It is therefore recommended that the State of Israel encourage the defense industries to invest in developing air defense solutions against UAVs of various sizes and types. One example is the transaction signed by Rafael Advanced Defense Systems with the United Kingdom for exporting systems against drones.[47] This system is likely to form an important export commodity in its own right, which will provide a response to a growing global challenge, while also aiding in the defense of Israel's security.

Investing in the development of means of defense against UAVs is also crucial because of the civilian use of UAVs, which is likely to expand greatly in the coming decades. This development will pose challenges not only to air defense but also to the air traffic management in any country that wishes to remain on the technological cutting edge and facilitate the operation of such systems in its territory for commercial and private needs, as well as those of the state itself.

In order to preserve exports, which helps to aid in the development of new systems, Israel should emphasize its other advantages and not just the technology. In this framework, Israel can also offer services to various countries and—more importantly—knowledge based on its operational experience and high quality personnel, as it did in its transaction of UAVs with Germany. This transaction includes nine-year leases (in contrast to purchasing) for Israeli Heron TP UAVs made by IAI Germany's military

47 Yuval Azulai, "Rafael to Sell 6 Anti-Drone Systems to UK for $20m," *Globes*, August 16, 2018, https://en.globes.co.il/en/article-rafael-to-sell-6-anti-drone-systems-to-uk-1001250393.

forces. In this framework, German teams will also be trained in Israel to operate the UAVs.[48] This method will make it possible to preserve strategic partnerships and create new ones.

Israel's strategic relations with India, which is significantly affected by the export of military technology, including advanced UAVs, is another example.[49] These relations indicate that exports of UAVs are more important than just the revenue generated. Israel should therefore continue investing in technological innovation and in the ability to provide solutions for the operational and technological needs of its clients, while manufacturing and exporting on relatively short timetables. In doing so, Israel will maintain other advantages beyond the prices of its products, which are not cheap in comparison to China or other competitors. Israel should also consider the possibility of providing support and sharing operational knowledge as part of the service for its clients, an advantage that many of its competitors are unable to offer.

Despite the growing competition in the international arena due to new players in the market and increased efforts by veteran players like the United States to expand their sales, Israel should carefully select the countries and regimes to which it exports military technologies, including UAVs, as it has done until now through the Israeli Defense Export Controls Agency (DECA). It should continue to do so even as new systems enter the market, such as civilian drones that provide a response to some of the existing military needs and do not require the use of military UAVs, or even constitute weapons in the hands of terrorist organizations.

Given the difficult competition in the military UAVs sector and the harsh criticism accompanying it on the one hand, and the huge economic potential in the civilian UAV market on the other,[50] Israel should consider increasing state investments in developing and manufacturing technologies for civilian needs, based on the relative advantage and knowledge that it has accumulated in the field of military UAVs. By this, the state will support

48 Assaf Uni, "Bundestag Approves €1b Israeli UAV Deal for German Army," *Globes*, June 13, 2018, https://en.globes.co.il/en/article-bundestag-approves-%E2%82%AC1b-israeli-uav-deal-for-german-army-1001241320.

49 Manu Pubby, "India all Set to get Missile Armed Drones from Israel," *Economist Times*, July 14, 2018, https://economictimes.indiatimes.com/news/defence/india-all-set-to-get-missile-armed-drones-from-israel/articleshow/57980098.cms.

50 Diamond, "Global Drones Market Expected to Surpass $22b by 2022."

the creation of another important export commodity, which is likely to also become a key source of revenue and an incentive for strategic partnerships with additional countries.

Israel should continue monitoring developments in the UAVs debate in the international arena, primarily in the various UN agencies, and try to utilize diplomatic means to prevent restrictions from being imposed on Israel in this field. Israel should also consider increasing its level of transparency regarding some of its own use of UAVs in order to avoid international criticism and its effects, including any politically motivated efforts by countries at the UN to restrict the use of attack UAVs, thereby damaging Israeli exports. Greater transparency will make it possible to ratify and validate the fact that Israel uses UAVs in accordance with the prevailing norms and international law, as well as to prevent attacks against it by human rights organizations and various countries. Increased transparency also may help portray Israel's capabilities in a positive light, which can also generate demand for those capabilities among other countries in the world.

Conclusion

Israel is one of the world's leading UAV exporters, and it is also one of the most prominent users of these systems and has many years of experience in operating them. Israel has faced challenges in recent years due to changes in the global proliferation of UAVs both in technological terms and due to the entry of new players into the market and a change of policy by veteran players. These developments pose a stiff challenge to Israel in terms of trade. Furthermore, the global proliferation of UAVs and the new aerial threats that these systems pose are a security challenge for Israel.

This article described Israel's dominance in the UAV sector, especially since the beginning of the twenty-first century, and the changes that have occurred over the past decade in the proliferation of UAVs throughout the world and in their use. The fact that China has become a major exporter and has a permissive export policy has caused far-reaching transformations in the entire international arena that also affect Israel. The challenges posed by Iranian UAVs and the extensive use of UAVs in the unstable Middle Eastern arena were also raised here. In addition, the entry of new players into the unmanned aircraft sector and the change in policy among veteran players in this area, such as the United States, poses trade threats to Israel.

Israeli policy can and should be adjusted to the changes taking place in the UAV sector. In this framework, this article proposed a series of measures: worldwide intelligence tracking of the spread of UAVs and their components, development of cyber and electronic warfare systems for countering the UAV threat, and adapting and upgrading Israel's air defense systems to deal with the new threats. It is also recommended that Israel step up its level of transparency with respect to UAVs, while at the same time it should carefully select the parties to whom it exports weapons. Israel should also consider additional ways to preserve and even increase its exports of unmanned aircraft. It should maximize the strategic achievements made possible by these exports and simultaneously consider the possibility of encouraging Israeli industries to develop UAVs for civilian needs and defense systems against UAVs due to the enormous economic potential in these markets and as part of the goal of preserving Israel's strength and security.

Lectures by **Lt. Gen. Gadi Eisenkot and Professor Yaël Ronen** on October 24, 2018

at a conference sponsored jointly by INSS and the Academic Center for Law and Science in Hod Hasharon to mark the publication of *Cyber Regulation* by Gabi Siboni and Ido Sivan-Sevilla

Operations in Cyberspace from the Perspective of International Law

Yaël Ronen

International law is applicable to cyberspace. There is international consensus that the UN Charter, which prohibits the use of force, applies to cyberspace. There is, nonetheless, some disagreement on what would constitute an armed attack in cyberspace, and consequently, what response would be permitted. Actions that do not amount to attack may still be prohibited by international law, for example if they constitute interference in the domestic affairs of states.

Keywords: Armed attack, international law, cyberspace, self defense

The debate on the regulation of cyberspace emphasizes the defense of this sphere. Discourse in international law regarding cyber activities differs from this debate in a number of respects: First, international law deals primarily with inter-state relationships rather than with domestic ones. Second, regulation is an act of organization, surveillance, and enforcement, which is intended to enforce binding rules of behavior. The basic assumption of regulation is that rules of behavior do exist; in contrast, international law is still at the stage of clarifying what rules exist or would be desirable with regard to cyberspace; or in other words, which acts are permissible and which are forbidden in this sphere. Third, whereas domestic regulation

Yaël Ronen is a professor of international law at the Academic Center for Science and Law in Hod Hasharon; and a research fellow at the Minerva Center for Human Rights at the Hebrew University in Jerusalem.
This article is based on a presentation given on October 24, 2018 at the Institute for National Security Studies, in collaboration with the Academic Center for Science and Law, marking the launch of the publication of *Cyber Regulation* by Colonel (res.) Dr. Gabi Siboni and Ido Sivan-Sevilla.

ordinarily focuses on **defending** cyberspace, international law focuses with the implications of the use of cyberspace for **attacks**.

Cyberspace activity poses a challenge for international law. First, international law in almost all its branches, regulates relationships involving tangible objects, whereas cyberspace is intangible. As a result, the question arises whether existing norms of international law are applicable to cyberspace, or rather it is necessary to draft new norms. Second, international law is based specifically on territorial divisions: The global arena is split into territorial units, namely states, and great emphasis is placed on the division of powers and privileges as embodied in the concept of sovereignty. In contrast, cyber activity inherently crosses borders. Third, international law is traditionally based on the primacy of states as actors: Those have rights, and they bear responsibilities. It seems that with respect to cyber activities, states are not the central actors.

These differences raise a basic question: Does international law apply to cyberspace? This question has been addressed primarily within academia. The First Tallinn Manual, a document drafted by a team of scholars and published in 2013, focused on the question of how international law can be applied to cyberspace, first and foremost in relation to the prohibition on the use of force and to the right of self-defense, as well as to actions that occur within the context of an armed conflict. The Second Tallinn Manual of 2017 expanded the debate to the applicability of international law to activities that do not involve the use force or do not amount to armed conflict. The formal involvement of states in this debates remains limited, in part because technology allows penetration into sensitive areas on which governments are reluctant to speak out; nonetheless, a consensus exists today that international law also applies in cyberspace. One of the notable developments in this context is the consensus reached in 2015 by an inter-governmental group of experts, which reached agreement that the UN Charter applies in its entirety also to cyberspace. This group included, among others, experts from the United States, Britain, Russia, and China, states which constitute the major players in the international arena. The consensus reached has several implications, some of which will be discussed below.

The UN Charter enshrines the prohibition on the use of force and on threats to use force against the independence or the territorial integrity of states and declares that use of force would only be legal when carried out in

self-defense or by authorization by the Security Council, and in exceptional circumstances. The question, of course, is what is considered "use of force" in the context of cyber activity. In this regard, cyber activity refers to actions against computer systems intended to gather, infiltrate, alter, or disrupt information through various means, or to manipulate network operations. It is widely agreed that a cyber activity may be considered "use of force" or an "armed attack" if its expected consequences are comparable to those of a kinetic attack or, in other words, can cause death or injury to people and damage to property. For example, cyber activity that results in a train derailment or the breach of a water main in a populated area would be considered an armed attack, just as if the train tracks had been subject to an aerial bombardment.

An example of this type of attack was the Stuxnet incident. In 2010 a malicious computer worm ("Stuxnet") infiltrated the systems that formed the basis for the centrifuges at one of the nuclear facilities in Iran, and caused the centrifuges to spin out of control and self-destruct. This was one of the first times that a cyber operation led to the physical destruction of an object. The action demonstrated the potential destruction and harm that cyber activities can cause, just like attacks through conventional means.

Classifying an act as an "armed attack" is significant because under certain circumstances, an armed attack entitles the victim state to use force in self-defense. If cyber activities may be considered armed attacks, then a forcible response is also conceivable. From this perspective, the Stuxnet worm attack on Iran might have given rise to a right of self-defense. An important question would then have arisen: Against whom is the injured party entitled to defend itself? Stakeholders in Iran and other states have accused the United States and Israel of being behind the Stuxnet attack, although there has been no real evidence indicating the involvement of any specific state in developing and spreading the worm. Another question is which measures would meet the standards of necessity and proportionality required in order for the response to be considered legitimate within the framework of the right of self-defense.

The most complex problem, over which there is still considerable disagreement, relates to situations in which cyber activities cause severe and substantial non-tangible damage. The conventional interpretation is that acts of collecting, stealing, or even destroying or altering information are not

considered armed attacks in and of themselves. Accordingly, armed response is not permissible. Nonetheless, the negative effects of such acts might be quite substantial. An example would be a cyberattack on economic or financial institutions, such as the New York Stock Exchange, which might cause the stock exchange to crash when the trustworthiness of its data and computer infrastructure is compromised. The question that arises in this context is whether the damage is purely economic, or whether the catastrophic results of the cyberattack justify categorizing it as an "armed attack."

This kind of cyber act was actually the trigger for interest in the applicability of international law to cyberspace: In April 2007 the government of Estonia declared its intention to move a World War II memorial from the center of its capital Tallinn to a military cemetery in the suburbs. Estonian citizens of Russian ethnicity reacted to this plan by violent protest. Subsequently, for about a month, internet infrastructure in Estonia was subject to attacks. The internet is a tool of preeminent usefulness in Estonia; 95 percent of banking transactions are digitized, and 98 percent of Estonian territory is connected to the internet, to the point that it is said that in Estonia the internet is almost as important as running water. The attacks on Estonia's internet infrastructure targeted the websites of the president, prime minister, parliament, political parties, banks, public media, and more. As a result, two major domestic banks were shut down for several days, and some of the central news agencies were damaged; emergency lines were disconnected for an hour; private and public communications were harmed; and most of all, faith in the national economy faltered. The attacks have been commonly linked to Russia, and some of them indeed were produced by computers controlled by Russian government institutions. However, the sources of the attacks were traced to 177 other countries, and most attacks originated from privately owned computers.

Estonian politicians compared the attacks to an invasion and to use of conventional military operations, but the actual damage incurred was limited and primarily economic: No harm was caused to property or lives; soldiers were not sent to the frontline; and there was no use of conventional weaponry. The basic economic infrastructure of the state, however, was damaged, crippling its ability to function.

The assertion that a state that falls victim to a substantial cyberattack may not respond through military means is very problematic. Disregarding

technological developments is likely to lead to absurd results and it is unlikely that states will abide by a rule that is inconsistent with realistic needs. Therefore, academics today widely agree that it is justifiable to categorize cyber activities that may cause severe consequences as "armed attacks." The question is what criteria are used to evaluate severity. Several elements may be taken into consideration, such as the repercussions to vital national interests, the immediacy of the outcome and the degree of its directness, the level of intrusion, and the level of state involvement.

Another principle anchored in the UN Charter is the prohibition on interfering in domestic issues of other states. This prohibition does not refer to specific methods and therefore also applies to interference by cyber means. The prohibition on interfering in domestic affairs is usually not prominent in international discussions, because when a conventional attack is waged on a state, the element of "interference" becomes a relatively minor issue. It is precisely when there is no recourse to violence, but rather to social or economic manipulations, that the prohibition on interference becomes a central issue.

As a rule, an act is considered to be "interference" when there is coercion or pressure, overt or otherwise. For example, espionage and data collection from computers in foreign countries are not considered interference, because even though there is an element of infiltration into a foreign computer network, these acts do not constitute coercion or the exertion of pressure on that country. The situation is different in the case of manipulating election results or public opinion via computers on the eve of elections. In some areas, the disagreement over classification is even greater: For example, what is the law regarding damage inflicted upon a political campaign of a specific party via content sites or the creation of fictional activities intended to sway public opinion? Arguably such actions constitute interference in the core of the state's sovereignty, albeit through political and social action rather than military; regardless, the effect may be quite severe. There is no doubt that these types of acts are illegal; what is an open question is how the injured state is allowed to respond.

Activity in cyberspace creates additional challenges for international law, such as the limitations on the use of cyber due to humanitarian legal principles and the risks that the use of cyberspace poses for the protection of human rights. International law has only just begun to engage with

these issues. The need to cultivate and hammer out norms in response to technological developments is not unique to international law; moreover, there is no doubt that basic legal principles of international law are present and exist also within cyberspace.

Cyberspace and the Israel Defense Forces

Gadi Eizenkot

Over the past decade, the Israel Defense Forces (IDF) has made the greatest strides in the field of cyberspace. During this period, cyberspace became a pertinent issue and in the IDF it became an extensive field of activity of developing and applying knowledge. The IDF perceives cyberspace and cyber regulation as significant for several reasons: First, they relate to the public discourse on knowledge development and the regulation of relations between the state and the economic system on the issue of national cyberspace and its resilience and the strengthening of the state's ability to continuing functioning in any emergency and while under enemy attack; second, cyberspace has great importance also in the international context. The State of Israel sees itself as being at the global forefront in developing cyber knowledge and, as such, can meaningfully contribute to developing the defense of cyberspace in other nations as well.

The IDF deals intensively with cyberspace and allocates significant resources for that purpose. Work in this field consists of three main components: first and foremost is defending military cyberspace and helping to secure civilian cyberspace. The IDF invests vast resources in fortifying cyberspace security. The second component concerns the army's ability to gather intelligence in cyberspace. As a result of technological development, increasing amounts

Lt. Gen. Gadi Eizenkot is the chief of the General Staff of the Israel Defense Forces. This essay is based on Lt. Gen. Eizenkot's lecture on cyberspace in the IDF given on October 24, 2018 at the conference jointly sponsored by INSS and the Academic Center for Law and Science in Hod Hasharon to honor the launch of *Cyber Regulation*, written by Dr. Col. (res.) Gabi Siboni and Ido Sivan-Sevilla.

of critical intelligence information is digitalized. Consequently, many more attempts at technological intelligence gathering efforts take place in cyberspace. The third component is cyberattacks—that is, the ability to make real operational gains via activity in cyberspace. The IDF integrates all these activities in its extensive operations.

Cyberspace as Part of the Threat Circle

The IDF is a very technological army, certainly when compared to some of Israel's enemies, and defense is viewed as critical to its functional capability. Since the establishment of the state, the IDF has faced three central threat circles, to which a fourth has been added in recent years. The first is the conventional threat from states with militaries of varying capabilities, including armored corps, infantry, and artillery, all capable of ground maneuvers, and supported by aerial offensive forces, aerial defense forces to disrupt IDF activity, and even maritime forces. All of these were constructed primarily for offensive goals in order to seize parts of the State of Israel.

The second longstanding threat circle against Israel is the nonconventional threat, which consists primarily of attempts by various regional parties to develop offensive military nuclear capabilities. This is evidenced by the Iranian vision of developing nuclear arms and by the Syrian efforts, foiled in 2007, to do so. Other such attempts may come to light in the future. In addition to nuclear weapons, some of the nations surrounding Israel have the capacity to engage in chemical warfare. Syria, for example, clearly possessed that capacity and, although it was significantly reduced five years ago, chemical warfare has been used several times during the Syrian civil war.

The third threat circle that has greatly preoccupied the IDF in the last decade and will continue to do so in the foreseeable future is the sub-conventional threat posed by terrorist and guerilla organizations operating against Israel. This threat consists, inter alia, of high trajectory fire on a large scale, having greater impact and accuracy than ever before, and the development of subterranean capabilities, both for defensive purposes for survival and offensive ones for penetrating into Israel in order to carry out terrorist attacks against Israeli settlements. In addition, the IDF and the other security organizations face threats by jihadist organizations and the attacks by individuals. The terrorist threat exists in Israel's north, south, and in Judea and Samaria, as well as toward Israeli and Jewish targets abroad.

The fourth threat circle is the cyber one. Aimed primarily at Israel's functional capabilities, both military and civilian, this is a relatively recent threat, which has expanded exponentially over the last decade and is expected to grow significantly in the coming years. Over the years, the IDF focused on developing warfare capabilities in three dimensions—land, sea, and air. In recent years, it has also started to develop warfare capabilities in the fourth dimension—cyberspace—with the understanding that this dimension needs to be addressed broadly and comprehensively, with preparations made at both the national and security levels. In its process of developing its knowledge, the IDF examines how to secure military cyberspace as well as state cyberspace, in the understanding that the IDF is charged with the responsibility of protecting security infrastructures, critical installations, economic capabilities, hospitals, airports, the banking sector, and so on, while at the same time protecting its military capabilities so as to allow the army optimal functioning in operating its command-and-control systems. These capabilities obviously depend on the most advanced means, including weapons and intelligence systems and aerial and naval capabilities.

The IDF in Cyberspace

The IDF's intensive work in cyberspace began about a decade ago. In recent years, the army has conducted a thorough study of the most suitable approach to developing and organizing this field. The IDF is not the only military doing so. Other nations, too, are examining the issue; the US military held comprehensive inquiry of the cyberspace question, which subsequently led the United States and Israel to share knowledge about the optimal way to organize military activity in cyberspace. The discussion hinged primarily on the best way to organize the defensive/security capability, the intelligence gathering capability, and the attack/offensive capability.

The IDF's learning process began about four years ago, with the learning and work of the general staff continuing for about a year. The question raised was how to properly organize. Several options were examined. Some required quite a leap, such as organizing all the military's cyberspace capabilities under one command; other were more conservative. Given that the IDF continuously and intensively deals with a broad spectrum of threats, it was finally understood that it would be improper to engage in a move that would be considered a step forward, with much trial and error in

a truly critical sphere of operations, especially since the security situation could quickly escalate. Given this, it was decided to progress gradually, using a measured approach to cyber organization in the IDF. As a result, the Computer Service Directorate's authority was expanded and its name changed to the CC4I Directorate. The Cyber Defense Division, whose personnel have a background in offense, was formed within this framework. At the same time, it was decided to reorganize the Military Intelligence Directorate, while unifying its intelligence gathering capability with other capabilities, with the understanding that the infrastructure of Unit 8200 and other infrastructures required in cyberspace must operate in an integrative manner. We expect that the progress and experience in this will lead ultimately to defensive, intelligence gathering, and offensive capabilities all united under one command.

In the United States, too, the relevant authorities are deliberating on the right way to be prepared in cyberspace and are considering splitting USCYBERCOM and the National Security Agency (NSA). As noted, the shared dilemmas have led to sharing information between the IDF and various US cyberspace entities, and we can assume that the process will continue for many years during which the current split model of handling different cyberspace fields will still be in effect. Nonetheless, at a certain point down the road, conditions and capabilities will reach the point where it will be possible to unite the entire cyberspace sphere under one command. It can be assumed then too that the move will be done in a measured, deliberate way.

The IDF has made a significant change in selecting and training personnel, and in its digital infrastructures, force building, and software houses. The changes in these fields and the enhancement of the Computer and IT Directorate have generated real reforms and upgraded the IDF's defensive capabilities in the cybersphere. In this context, the enhancement of the IDF's telecommunications abilities as part of the Digital Ground Army project is remarkable; more than 10 billion NIS were invested in order to provide the IDF's ground forces with better functionality and optimization in concentrating information about the enemy, the IDF, and the combined use of IDF force. The reorganization carried out in the Military Intelligence Directorate led to a fundamental change within its systems aimed at optimization and reducing duplications. Significant changes and enhancements were also made to

inter-organizational integration and cooperation among the IDF, the General Security Service, and the Mossad, as well as to capabilities at the state level.

The IDF holds quite a few joint drills and training exercises within its own framework as well as with other organizations—including foreign militaries—to learn and share cyber information, having understood that this developing challenge requires the sharing and exchange of information. The IDF also actively participates in drills and capacity building in order to secure the state in emergencies conducted in close cooperation with the National Cyber Directorate. This aspect of the IDF's work stems from the fact that it views itself as an inseparable part of defending and protecting the national cyberspace in emergencies and wartime. To do this, it is necessary to continue developing knowledge and a common language among all the branches of the State of Israel, in addition to and beyond the great progress made in the field to date. The unknowns in this field still outnumber the knowns, and that is the way it ought to be.

Conclusion

The IDF has made tremendous strides in its Digital Ground Army plan, allowing modern commanders at all ranks to get more information and generate more up-to-date assessments of the enemy's location and the IDF's own forces in the field. This progress, however, is liable to cause an overload of information for the field ranks, which could cause greater harm than good. It should be remembered that too much information is not a guarantee for better command and control. The IDF has analyzed all of this, and it is important to be cognizant of this: "[If] in the past the tactical commander fought to get data about the location of his troop and the location of the enemy so that he could make decisions, today these data—as well as many other data—are presented to him. As a result, he now faces a new challenge: to sort the chaff from the wheat and find the relevant details of the information that will allow him to make better decisions and obtain a decisive victory in the fighting."[1]

Progress and transparency of information have other psychological implications on the way that commanders share information. As Clausewitz

1 Gabi Siboni and Moran Mayorchik, "The Curse of Abundance," *Ma'arakhot* 459 (February 2015): 19 [in Hebrew].

said, war is the realm of uncertainty and thus it will ever remain.[2] It is therefore important that transparency of information not confuse the various ranks during the decision-making process and that the ranks of command be maintained. The fact that the entire chain of command—the company commander, the battalion commander, the brigade commander, and the division commander—sees all the information at the same time should not cause a Tower of Babel situation; the advanced command-and-control systems, which enable everyone to see the same information, must not be allowed to lead to a situation in which a division commander or head of a command act as if they are at the level of company commander and think they understand the situation better and can therefore make better decisions than those who are actually in the field.

The IDF will continue to develop in cyberspace, build capabilities, organize the commands, and develop new technological tools. But in tandem with technological progress, which is a force multiplier for the IDF compared to its enemies, it is extremely important always to retain the fundamental principles and approaches of the command. These, based on thousands of years of human experience, are not merely conservative tenets; on the contrary, they do a better job of arranging the way in which the art of war is manifested on the battleground, the way decisions are made, and the processes of their implementation.

Military activity will continue to require difficult and demanding physical efforts. The days of sterile fighting with buttons alone still lies far ahead in the future if it should ever come. Therefore, even though the IDF is making tremendous efforts in developing its cyber capabilities, the need to maintain and develop its kinetic abilities has not changed, because the wars of the future will continue to be decided on the physical battlefield.

2 Roger Ashley Leonard, ed., *A Short Guide to Clausewitz on War* (Tel Aviv: Ministry of Defense, 1977), p. 79 [in Hebrew].

Cyber, Intelligence, and Security

Call for Papers

The Institute for National Security Studies (INSS) at Tel Aviv University invites submission of articles for ***Cyber, Intelligence, and Security***, a new peer-reviewed journal, published three times a year in English and Hebrew. The journal is edited by Gabi Siboni, head of the Cyber Security Program and the Military and Strategic Affairs Program at INSS.

Articles may relate to the following issues:

- Global policy and strategy on cyber issues
- Cyberspace regulation
- National cybersecurity resilience
- Critical infrastructure cyber defense
- Cyberspace force buildup
- Ethical and legal aspects of cyberspace
- Cyberspace technologies
- Military cyber operations and warfare
- Military and cyber strategic thinking
- Intelligence, information sharing, and public-private partnership (PPP)
- Cyberspace deterrence
- Cybersecurity threats and risk-analysis methodologies
- Cyber incident analysis and lessons learned
- Techniques, tactics, and procedures (TTPs)

Articles submitted for consideration should not exceed 6,000 words (including citations and footnotes), and should include an abstract of up to 120 words and up to ten keywords. Articles should be sent to:

Hadas Klein
Coordinator, ***Cyber, Intelligence, and Security***
Tel: +972-3-6400400 / ext. 488
Cell: +972-54-4510411
hadask@inss.org.il