Cyber, Intelligence, and Security

Volume 2 | No. 1 | May 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. 1 | May 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.

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

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

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

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

When Less is More: Cognition and the Outcome of Cyber Coercion

Miguel Alberto Gomez

The rise of offensive interstate cyber interactions continues to fan interest in the coercive potential of cyber operations. Advocates of this revolutionary view insist that it signifies a shift in the balance of interstate relations; yet empirical evidence from past cases challenges these beliefs as actions often result in continued resistance rather than compliance. Regardless of its performance, the coercive potential of cyber operations cannot be readily dismissed. Consequently, the paper advances that the outcome of coercive cyber operations is better explained using heuristic decision-making strategies rather than normative approaches such as expected utility.

Keywords: Cognitive heuristics, expected utility, coercion, cyberspace

Introduction

On December 23, 2015, a cyber operation disabled over fifty power substations in western Ukraine leaving over 230,000 residents without electricity. This incident marked the first case of a cyber incident resulting in the disruption of a state's power grid.[1] With the Ukrainian-Russian conflict well into its third year, the notion that similar events serve as adjunctive coercive tools in times of dispute is further reinforced.[2]

Miguel Alberto Gomez is a senior researcher at the Center for Security Studies, ETH, Zurich and a PhD candidate at Cardiff University, Wales.

1 Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *WIRED*, March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

2 SANS-ICS, "Analysis of the Cyber Attack on the Ukrainian Power Grid," *SANS*, March 18, 2016, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

Building on propositions from several authors, the rate at which politics, the economy, and the larger global society are increasingly dependent on cyberspace potentially magnifies the perceived threat.[3] This appears to empower the exercise of cyber coercion by increasing the potential cost of non-compliance with threats against the underlying cyber infrastructure. Yet despite these claims, such cases have performed poorly, with adversaries opting to resist rather than comply with an aggressor's demands.[4] Furthermore, even technically advanced operations have not resulted in significant policy shifts.[5] While critical voices attribute its lackluster performance to inherent domain limitations, the strategic utility of cyber coercion should not be readily dismissed. As noted by Gartzke and Lindsay, "the potential of cyberspace is more limited than generally appreciated, but is not negligible."[6] Thus, the continued use by states of coercive cyber operations merits further inquiry.

Consequently, this paper shifts away from the prevailing view that the success or failure of coercive cyber operations results from normative decision-making strategies through which the decision to comply or resist is a function of expected gains or losses. Instead, cognitive heuristics offers a clearer insight as to why states behave as they do contrary to the expectations of "more rational" strategies. While the parsimonious account offered by variants of the rational choice paradigm simplifies our understanding of this complex environment, the inclusion of a cognitive dimension reflects the need to seek narratives that better illuminate the phenomenon of cyber coercion. In so doing, the paper acknowledges the urgency raised by Dean

3 Myriam Dunn-Cavelty, "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse," *International Studies Review* 15, no. 1 (2013): 105–122; Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (2013): 365–404; Jon R. Lindsay and Erik Gartzke, "Coercion through Cyberspace: The Stability-Instability Paradox Revisited," in *The Power to Hurt: Coercion in the Modern World*, ed. Kelly Greenhill and Peter Krause (New York: Oxford University Press, 2016).

4 Benjamin M. Jensen, Brandon Valeriano, and Ryan Maness, "Cyber Victory: The Efficacy of Cyber Coercion," (Paper presented at the Annual Meeting of the International Studies Association, Atlanta, GA, 2016).

5 Emilio Iasiello, "Cyber Attack: A Dull Tool to Shape Foreign Policy," in *Fifth International Conference on Cyber Conflict*, ed. Karlis Podins, Jan Stinissen, and Markus Maybaum (Tallinn: NATO CCDCOE, 2013), pp. 451–468.

6 Lindsay and Gartzke, "Coercion through Cyberspace."

and McDermott that an understanding of state behavior in cyberspace rests on the interaction of factors across different operational levels.[7]

Therefore, the paper serves as a plausibility probe to demonstrate the suitability of cognitive heuristics as a valid decision-making strategy in response to coercive cyber operations. In so doing, the paper is divided into four key sections. The first provides a brief overview of coercion in the context of cyberspace. This is followed by a critique of the prevailing account that cyberspace is a domain of risk that results in the misaligned application of expected utility in interpreting state response to cyber coercion. In its place, cognitive heuristics is offered as a viable alternative with the understanding that decisions emerge from the exploitation of the unique statistical characteristics of cyberspace using frugal cognitive processes. The suitability of this approach is then explored through a plausibility probe of the Stuxnet campaign. Finally, the paper concludes with the possible limitations of this theoretical framework.

Coercion and Cyberspace

For the past two decades, strategic interest in cyberspace has been encouraged by the growth and pervasiveness of the underlying cyber infrastructure.[8] These developments, however, are overshadowed by fears of exploitable vulnerabilities within these systems and sub-systems that reinforce the belief of aggressors employing denial or punishment strategies with coercive intent.[9] This highlights the domain's inherent vulnerability relative to its socio-political and economic value, thus portraying a future in which exercising cyber power—manifested in cyber operations—serves as a principal coercive instrument for actors capable of employing it. As coercion is defined as the

7 Benjamin Dean and Rose McDermott, "A Research Agenda to Improve Decision Making in Cyber Security Policy," *Penn State Journal of Law and International Affairs* 5, no.1 (2017).

8 Stuart Starr, "Toward a Preliminary Theory of Cyberpower," in *Cyberpower and National Security*, ed. Franklin Kramer, Stuart Starr, and Larry Wentz (Washington DC: Potomac Books, 2009), pp. 43–88.

9 Robert A. Pape, *Bombing to Win: Air Power and Coercion in War* (New York: Cornell University Press, 1996); John Stone, "Cyber War Will Take Place!" *Journal of Strategic Studies* 36, no. 1 (2013): 101–108.

use or threat of force to elicit a change in an adversary's behavior,[10] the above conditions validate the employment of cyber operations for this task. Given that the outcome is a function of possible losses or gains, threats to the underlying infrastructure that support a state's strategic interest lead to a re-evaluation of an adversary's position.

While the study of coercion in cyberspace has and continues to attract academic interest, the available literature remains scarce. Initial studies indicating the coercive potential of cyber operations reflect its purported offensive advantage. Saltzman writes that this advantage is enabled by the versatility and "byte power" of the cyber operations. He argues that versatility is the ability of actions in cyberspace to negatively impact a state's strategic interests.[11] Byte power, in turn, is the amount of damage inflicted by actions in cyberspace. Apart from these, the perceived absence of material constraints also grants cyber operations an asymmetric advantage. While access to advanced conventional (and nuclear) weapons is often constrained by economic considerations, the availability of tools via underground networks presumably offer materially deficient aggressors an advantage; yet, despite these arguments, the outcome of past cases calls into question the coercive potential of cyber operations.

Out of 164 past operations that were identified, only 64 percent resulted in observable changes of an adversary's behavior.[12] Furthermore, attempts to compel an adversary through denial were only successful approximately 1 percent of the time. If the underlying domain conditions—in conjunction with the offensive advantage offered by cyber operations—does indeed enhance the coercive potential of cyber operations, then what accounts for its dismal success rate?

Coercive Success or Failure

While the evidence suggests the limited potential of coercion through cyberspace, it does not completely discount its utility. Although the need to set expectations is merited, the factors that give rise to coercive success or

10 Daniel Byman and Matthew Waxman, *The Dynamics of Coercion: American Foreign Policy and the Limits of Military Might* (New York: Cambridge University Press, 2002).

11 Ilai Saltzman, "Cyber Posturing and the Offense-Defense Balance," *Contemporary Security Policy* 34, no. 1 (2013): 40–63.

12 Jensen, Valeriano, and Maness, "Cyber Victory: The Efficacy of Cyber Coercion."

failure in cyberspace remain unidentified. For studies concerning the exercise of coercion, expected utility theory is routinely employed to evaluate state behavior. It posits that an actor's decision to resist or comply is based on the maximization and minimization of gains and losses relative to their net position. As states continue to invest in cyberspace to meet strategic objectives, coercive threats are increasingly being leveled against economic, political, social, or military goals, with the decision to comply or resist due to the (threat of) disrupting these goals.[13]

The prevailing factor supporting the coercive potential of cyber operations is the ability to exploit technological vulnerabilities.[14] A common threat representation within cyberspace is that of its vulnerabilities, unknowabilities, and inevitabilities exploited by cyber operations. Cavelty points to the conceptualization of threats originating from vulnerabilities and the extent to which systems deemed as "critical" are susceptible and adversely affected by them.[15] The interconnected nature of these systems allows individuals and organizations to continually innovate and extend their reach; however, it also magnifies the consequences in the event of exploitation. Given the complexity of these technologies and fundamental human limitations, eliminating these threats through improved product development and quality management is infeasible.

Consequently, these conditions introduce a chain of events that favors coercion through cyber operations. First is the loss of the sense of security. The complexity of the domain increases the possibility that an exploitable vulnerability exists. This fosters a notion of inevitability that an aggressor would discover this vulnerability and use it to its advantage. Finally, should this vulnerability be present in systems and sub-systems deemed as "critical," it potentially places a given society at risk.[16] In so doing, the application of expected utility theory to this scenario suggests that the likelihood of losses incurred due to coercive threats being exercised is relatively high and results

13 Starr, "Toward a Preliminary Theory of Cyberpower."

14 Ronald J. Deibert and Rafal Rohozinski, "Risking Security: Policies and Paradoxes of Cyberspace Security," *International Political Sociology* 4, no. 1 (2010): 15–32.

15 Dunn-Cavelty, "From Cyber-Bombs to Political Fallout."

16 Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly* 53, no. 4 (2009): 1155–1175; James Lewis, "National Perceptions of Cyber Threats," *Strategic Analysis* 38, no. 4 (2014): 566–576.

in compliance. The validity of this argument, however, rests not only on the recognition of this causal process and the probability of its realization but also on an adversary's ability to mitigate these threats. This presupposes that an actor in cyberspace exists in a risk-centric environment and possesses knowledge of threats, capabilities, and consequences.

The Cyberspace Environment

The literature on cyber coercion tends to conflate the notion of risk and uncertainty resulting in the inappropriate application of expected utility. Although the terms "risk" and "uncertainty" suggest a conceptual equivalency, each describes a unique information environment that influences the quality and processes of decision making. In adopting the terminology employed by Savage, risk refers to a "small world" in which the decision maker is aware of the probabilities of all possible outcomes and alternatives. In contrast, uncertainty reflects a "large world" where probabilities are not known or cannot be expressed with any mathematical certainty.[17]

If cyberspace is treated as a domain in which interconnectedness constrains the ability to predict possible points of failure and likely consequences, it then follows that decision makers operate in the context of uncertainty rather than in that of risk. In this respect, it has been shown that normative strategies (i.e., expected utility) employed in environments of uncertainty rather than risk often underperform. This issue is manifested through the bias-variance dilemma that is aggravated when normative strategies are applied to inappropriate environments.

The predictive accuracy of decision making is challenged by two important factors: bias and variance. The former refers to the extent to which a model deviates from the true state of the environment. As it is not possible to know the true state beforehand, a truly unbiased model cannot exist. The presence of bias, however, is mitigated by increasing variance through the addition of free parameters that accommodate a larger variety of true states. Doing so, however, risks overfitting and reduces predictive accuracy. Normative strategies such as expected utility offset bias with the inclusion of such parameters. This approach is suited to environments wherein exemplar cases

17 Kirsten G. Volz and Gerd Gigerenzer, "Cognitive Processes in Decisions Under Risk are not the Same as in Decisions Under Uncertainty," *Frontiers in Neuroscience* 6, July 12, 2012.

are readily available or where these cases are not ambiguous. Barring these conditions, normative strategies may be able to accurately describe previous observation but fail in predicting future outcomes; in this case, cognitive heuristics may prove to be better suited to this task.

Heuristics are defined as "strategies that ignore part of the information, with the goal of making decisions more quickly, frugally, and/or accurately than more complex methods."[18] Compared with their normative counterparts, errors in this approach emerge solely from bias. While it seems counterintuitive to suggest that accuracy is achieved with less information, these heuristics outperform their more "rational" counterparts when exercised in uncertain environments. Take the case of investments as an example. Borges and others demonstrate that mere recognition of a company's name can be employed to build an investment portfolio with returns that are least 10 percent greater compared to other strategies.[19] In their research, there appears to be a strong positive correlation between the company and its performance in the market that is exploited by decision makers using their ability to recognize this relationship from memory (i.e., recurring media coverage of a well-performing company). Consequently, this serves as a cue to pick one company over another when building a portfolio.

Although an in-depth discussion of heuristics is beyond the scope of this paper, it is crucial to point out that the advantages exhibited by heuristics rest on the ability to exploit the statistical characteristics of an environment using inherent cognitive capabilities such as memory. In other words, heuristics are only as accurate as the extent to which they fit existing structures.[20] This is otherwise known as ecological rationality.

---

18 Gerd Gigerenzer and Wolfgang Gaissmaier, "Heuristic Decision Making," *Annual Review of Psychology* 62 (2011).

19 Bernhard Borges, Daniel G. Goldstein, Andreas Ortmann, and Gerd Gigerenzer, "Can Ignorance Beat the Stock Market," in *Simple Heuristics That Make Us Smart*, ed. Gerd Gigerenzer, Peter M. Todd, and the ABC Research Group (New York: Oxford University Press, 1999).

20 Laura Martingnon and Ulrich Hoffrage, "Why Does One-Reason Decision Making Work?" in *Simple Heuristics That Make Us Smart*, ed. Gerd Gigerenzer, Peter M. Todd, and the ABC Research Group (New York: Oxford University Press, 1999).

The Ecological Rationality of Cyberspace

Environments in which heuristics are well suited to are characterized by uncertainty, redundancy, sparseness of data, and variability.[21] While earlier sections have touched upon the uncertain nature of cyberspace, this requires further elaboration. Extending Perrow's work on "normal accidents," it is argued that the connectivity and interdependency that cyberspace enables simultaneously curtails attempts to predict both the causes and effects of disruptive events. The possibility of a cascading disaster upon which the coercive potential of cyber operations is grounded would not exist without this paradoxical relationship.[22] Take, for instance, the case of a word processor. As a standalone application, security professionals are able predict the number of vulnerabilities per thousand lines of code based on their experience with similar software. In this situation, one operates in an environment of risk given the knowledge of possible vulnerabilities obtained from direct access to the underlying code and/or experience. To enhance productivity, however, users could interconnect their word processors to engage in collaborative work. In so doing, previous knowledge with respect to vulnerabilities is devalued since the state of other systems with which they connect are unknown. Consequently, it becomes difficult to predict where, when, or how failure could occur, thus placing users in an environment of uncertainty.

When applying this logic to the question of coercion, states that depend on these systems cannot predict the true extent or damage that aggressors may inflict. This inhibits an accurate assessment of the consequences of either complying or resisting coercive demands. While some argue that this, in fact, challenges the utility of coercion in cyberspace, this paper claims that this does not necessarily diminish the feasibility of cyber coercion; rather, it suggests instead that this lack of information influences the selection of an appropriate decision-making strategy when viewed in the context of other events.

Coercion in cyberspace does not exist in a vacuum and the underlying uncertainty is tempered by existing redundancies. Redundancy is the correlation between informational cues used in decision making. It is important to

21 Peter M. Todd, Gerd Gigerenzer, and the ABC Research Group, *Ecological Rationality: Intelligence in the World* (New York: Oxford University Press, 2011).

22 Charles Perrow, *Normal Accidents: Living with High-Risk Technologies* (Princeton: Princeton University Press, 1999).

note that coercive cyber operations often involve established rivals with a history of aggressive behavior toward one another.[23] As such, certain actions between parties are expected whether they manifest in the physical or virtual domain. Chinese cyber espionage toward the United States, for instance, is not particularly surprising and is positively correlated with China's interest in gaining an informational advantage. The WannaCry ransomware attack attributed to the North Korean regime, in contrast, does not appear to be related to their current strategic or political objectives. This demonstrates that certain events in cyberspace are framed by established interstate relations. Consequently, decision makers may exploit this relationship and their familiarity with these issues to evaluate coercive cyber operations and their consequences.

While cyberspace may be perceived as an extension of the physical domain where pre-existing relationship are continuously expressed, these events are quite rare. Therefore, information pertaining to the overall efficacy of coercive cyber operations, preferred tools and tactics, and other relevant information are sparse. Although advancements in forensic techniques have allowed a better analysis of technical characteristics, they alone provide limited strategic insight.[24] Consequently, the uncertainty that exists at the technological level is further compounded by uncertainty at the strategic/political level, thus casting greater doubt on the usefulness of coercion through cyberspace. This only appears to be the case, however, if viewed through the lens of normative approaches such as expected utility. Since decisions are made based on gains and losses, the scarcity of information should not confirm the absence of future losses nor the continued success of initial compromise since decision makers are not privy to all possible outcomes and alternatives.

Finally, the performance of heuristics depends on the weight or validity of cues within the environment. Validity is the rate by which cues can correctly discriminate between choices. For instance, has the forward deployment of ground forces in the past resulted in the compliance of the threatened state? Linking this to key tenets of coercion theory, the outcome of coercion is

23 Brandon Valeriano and Ryan C. Maness, "The Dynamics of Cyber Conflict Between Rival Antagonists, 2001–11," *Journal of Peace Research* 51, no. 3 (2014): 347–360.

24 Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1 (2015): 4–37.

dependent on both the ability of a coercer to exact costs on an adversary by threatening its assets and how the latter valuates those said assets. While the literature correctly assesses the first point of this argument, it rarely recognizes variations across adversaries with respect to their perception of cyberspace, which, in turn, influences the valuation of assets.[25] In other words, what may be a valid cue that predicts compliance in one case may not be the same with another, thus increasing uncertainty.

Heuristic Selection

The preceding section has established a case in which heuristics appear a viable alternative in explaining the outcome of coercion in cyberspace, given the domain's ecological rationality. First, uncertainty denies decision makers the ability to empirically assess all possible outcomes and alternatives. Second, the correlation between events in cyberspace and existing rivalries compensates for extant uncertainties and enables the use of similar cross-domain experiences to inform decisions. Third, the rarity of coercive cyber operations further inhibits the use of normative strategies as these deny decision makers points of references upon which to base their decisions on. Finally, the inability to recognize variations in cue validity results in an incorrectly specified approach. With these points in mind, the question that remains is which heuristic can best exploit these environmental structures.

The paper posits that one-reason heuristics provide insight regarding the outcome of cyber coercion. This family of heuristics performs well in cases where cue validities vary highly, significant redundancy exists, and data is scarce.[26] If this family of heuristics is employed in deciding whether to comply or resist coercive demands, the decision-making process proceeds in accordance with search, stopping, and decision rules. These rules govern the search of appropriate cues, the conditions that leads to the cessation of the search, and the way these cues are employed resulting in a specific decision.

As simple as heuristics may be, these have been shown to outperform more complex strategies such as multiple regression, neural networks, and so forth. However, it is important to establish that this strategy is non-

25 Forrest Hare, "The Cyber Threat to National Security: Why Can't We Agree," in *Conference on Cyber Conflict Proceedings*, ed. Christian Czosseck and Karlis Podins (Tallinn: CCD COE, 2010).

26 Gerd Gigerenzer, "Why Heuristics Work," *Perspectives on Psychological Science* 3, no. 1 (2008): 20–29.

compensatory in that it avoids looking for conflicting evidence and relies on a subjective rather than objective assessment of a given situation. This may prove to be troublesome, if not dangerous, in certain environments. For instance, a false flag operation by a third party that mimics the behavior of one rival may result in unintended escalation under the right circumstances.

The Viability of Heuristics: Stuxnet

To support the preceding theoretical arguments, the feasibility of heuristics is demonstrated with a plausibility probe. Although several events since 2007 may serve this purpose, the paper employs the often-used case of Stuxnet that has been attributed to both the United States and Israel. The decision to do so is due to the availability of information pertaining to this case that allows for a comparison of the two decision-making strategies to be made.

The interaction between the United States and Iran in cyberspace is characterized as a series of coercive acts of varying intensity, severity, and scope.[27] Of these, Stuxnet remains the most prominent case of cyber coercion. The existence of Stuxnet first came to light in June 17, 2010 when the Belarusian anti-virus company VirusBlokAda was approached to respond to unknown system reboots occurring in Iran.[28] Despite its "initial" discovery in 2010, analysts believe that it had been operational as early as June 2009 with ten initial infections affecting five organizations within Iran and resulting in a total of 12,000 infections by the time it was identified in 2010. Its advanced feature set suggests the involvement of state or state-funded organizations in its development and eventual release. This gave it the recognition as being the first "weaponized" malware in history. Moreover, its feature set and targets (Industrial Control Systems) signaled a shift in capability, complexity, and intent of actors within cyberspace.[29] By the time the infection had been contained, over 1,000 nuclear centrifuges used for

27 Jason Healey, "Winning and Losing in Cyberspace," in *Eighth International Conference on Cyber Conflict*, ed. Nikolaos Pissanidis, Henry Roigas, and Matthijs Veenendaal (Tallinn: CCD COE, 2010).

28 Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired*, March 11, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

29 Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (2013): 365–404.

uranium enrichment had been damaged, and the discourse regarding the use of cyber weapons had entered a new era.

Yet despite its operational characteristics, Stuxnet failed to coerce the Iranian regime in ending its nuclear enrichment program. The prevailing sentiment is that Stuxnet's failure stemmed from the limited damage inflicted against Iran's enrichment infrastructure. Post-incident analysis revealed that the number of centrifuges affected did not exceed normal operational wear-and-tear, and this account appears consistent with our understanding of coercion viewed through the lens of expected utility theory. In other words, the damage did not reach disruptive or debilitative levels that would prompt a reassessment of policy. Yet for this argument to hold, one must allow for one crucial assumption: that the Iranian regime had adequate knowledge of their capabilities and vulnerabilities in cyberspace, providing the confidence to risk further attempts against their cyber infrastructure. If true, this implies that the decision to resist was made in an environment of risk. The Iranian response, however, challenges this at an empirical and theoretical level.

While it is unreasonable to assume that those responsible for Iranian cyber security had perfect knowledge of all the possible attack vectors, a suitable security program would at least have taken steps to mitigate viable threats as informed by both first-hand experience and publicly available knowledge. Without direct involvement or insight into their internal processes, this readiness is deduced from behavior once a threat is realized. In the case of Stuxnet, reports that Iranian authorities had resorted to external third parties to better understand the unusual behavior of their systems suggests that a Stuxnet-like event had not been anticipated nor its consequences considered. Through no fault of their own, the complexity of Stuxnet had no precedence from which computations of possible losses could be derived.

Although it may be argued that additional information regarding the capabilities and damage potential of Stuxnet could have surfaced as the investigation proceeded, this implies the existence of both technological expertise and established organizational structures in support of such endeavors. Organizations require a mechanism that enables the synthesis of information across different units to understand the full implications of these events. Furthermore, the existence of such a structure cannot be

assumed across states nor is their efficacy a foregone conclusion.[30] Iranian dependence on external aid during the incident, along with earlier reports of their cyber capabilities, calls into question their ability to fully comprehend the consequences of Stuxnet and further challenges the applicability of normative strategies that explain their decision to resist.

Finally, if the Iranian regime was indeed confident in their ability to defend against Stuxnet or further acts of coercion, then why had there not been a stronger response? Both Gartzke and Lindsay argue that operations that result in compromise but are eventually contained end in an escalatory spiral.[31] Though less extreme, the game theoretic model of Edwards and others suggests that those aware of their vulnerabilities and who have mitigated them should at least publicly attribute coercive acts to their rivals.[32] Neither had transpired with respect to Stuxnet. Although some analysts claim that later Iranian cyber operations were such a response, their operational characteristics do not appear to be proportionate nor tailored to serve as a reply to Stuxnet.

The prevailing account of Stuxnet's failure, while seeming to confirm the usefulness of normative strategies, stands on unstable ground upon closer inspection. Although speculative without first-hand information, it appears that the Iranian regime did not have a full understanding of their own vulnerabilities. Consequently, it would not have been appropriate for decision makers to rely on expected utility or its related strategies to frame their response given that information regarding the possible consequences of resisting or complying were either incomplete or unavailable. Furthermore, the feasibility of normative strategies is challenged further in other cases of cyber coercion. The "BoxingRumble" operation against Chinese cyber espionage, for instance, did not result in significant damage either; nonetheless, Chinese operations were halted for the time being in response.[33] This apparent

30 Rebecca Slayton, "What is the Cyber Offense-Defense Balance?" *International Security* 41, no. 3 (2017): 72–109.

31 Erik Gartzke and Jon R. Lindsay, "Thermonuclear Cyberwar," *Journal of Cybersecurity* 3, no. 1 (2017): 47–48.

32 Benjamin Edwards, Alexander Furnas, Stephen Forrest, and Robert Axelrod, "Strategic Aspects of Cyber Attack, Attribution, and Blame," in *Proceedings of the National Academy of Sciences* (forthcoming).

33 Sean Gallagher, "NSA secretly hijacked existing malware to spy on N. Korea, others," *arsTechnica*, January 19, 2015. https://arstechnica.com/information-technology/2015/01/nsa-secretly-hijacked-existing-malware-to-spy-on-n-korea-others/.

contradiction appears to question the validity of conclusions established through normative strategies.

Filling the Gap

If normative strategies such as expected utility are not suited for this environment, would there be reason to believe that heuristics could do better? Extending the argument that cyber coercion occurs between rivals and that the environmental structures favor one-decision heuristics, this assumption is demonstrated using the "Take The Last" (TTL) heuristic.

The TTL heuristic functions by employing a strategy known as an *Einstellung* set. Psychologists since the 1930s have observed that individuals solve seemingly related problems with strategies that had worked in the past.[34] This assumes that the TTL heuristic is invoked in environments where decisions are frequently made about events that are correlated with one another in some form. This correlation is indirectly manifested in the ability of the decision maker to recognize similarities between different tasks; however, recognition in this case is not necessarily equivalent to memory but rather refers to the intuitive characteristics of events that are reinforced through constant exposure.

Since coercive cyber operations involve established rivals that routinely interact with one another, TTL is an ideal strategy not only because of environmental structures but also of its efficiency. Unlike expected utility that requires intensive computation, which increases cognitive load, TTL relies merely on recognition to identify alternatives. Furthermore, in time-critical situations such as interstate disputes, the speed with which TTL is exercised makes it a preferable choice over alternative strategies. Thus, TTL proceeds as follows: search for the cue that stopped the search during the last related problem; compare the validity of the cue relative to the alternatives. If it discriminates, use the cue; otherwise, go back to the problem before the last and determine which cue stopped that search.

In explaining the outcome of Stuxnet using the TTL heuristic, the process begins by building a repository of all the similar events in the past. Since

34 Gerd Gigerenzer and Daniel G. Goldstein, "Betting on One Good Reason: Take the Best Heuristic," in *Simple Heuristics That Make Us Smart*, ed. Gerd Gigerenzer, Peter M. Todd, and the ABC Research Group (New York: Oxford University Press, 1999).

the target of Stuxnet had been systems-controlling nuclear centrifuges responsible for enrichment, the repository most likely contained previous attempts to coerce Iran into stopping its nuclear program. This assumption is not necessarily tenuous given the amount of effort invested by its rivals who achieve just that. Furthermore, the fact that this occurred in cyberspace should not challenge the ability of decision makers to recognize similarities since the objective in question remains the same (i.e., ending the nuclear program).

Once this mental repository is constructed, the decision maker needs to identify the last instance when the cue discriminated between alternatives. Since first-hand accounts are unavailable, this paper turns to a timeline of coercive events prior June 2010. Despite the existence of on-going talks between 2006 and 2010, the United Nations Security Council imposed a total of six sanctions intended to disrupt the nuclear enrichment program. Apart from this, the United States had also begun to seriously consider air strikes while Israel threatened military action. While it is impossible to determine which of these events was used as a reference point, it should not matter since the outcome had been the same on the part of Iran: resist.[35]

Given that the context that framed Stuxnet and a similar event in the past, it is likely that decision makers opted to remain consistent with their defiant behavior. The characteristics of Stuxnet would have limited the accuracy of more complex decision-making strategies given the lack of information regarding its true capabilities and the extent of compromise. Furthermore, if resistance had worked when the threat was greater (i.e., thoughts of actual physical confrontation), then it should also suffice in this less extreme situation.

The Way Forward

Over the course of several pages, this paper has built an argument in support of cognitive heuristics as an analytical tool to evaluate the outcome of coercive cyber operations. Although normative strategies remain the mainstay for evaluating state behavior, the unique characteristics of cyberspace calls its adequacy into question. Whereas experience in the physical domain permits the objective evaluation of gains and losses, the uncertainty endemic to

35 Shreeya Sinha and Susan Campbell Beachy, "Timeline on Iran's Nuclear Program," *New York Times*, April 2, 2015, https://www.nytimes.com/interactive/2014/11/20/world/middleeast/Iran-nuclear-timeline.html?_r=0#/#time243_10809.

cyberspace limits the predictive accuracy of expected utility and related strategies. In its place, fast-and-frugal strategies such as Take The Last heuristic provide a more robust account of coercion in this virtual domain.

Depending on heuristics, however, is not a foregone conclusion. As there is no such thing as a one-size-fits-all decision-making strategy, the performance of either heuristics or normative strategies is a function of both environmental structures and individual cognitive capacities. This interdependence is best expressed in Herbert Simon's analogy of rationality as scissor blades where one blade represents the cognitive limitations of individuals while the other represents environmental structures and conditions. In as much as a pair of scissors cannot work with just one blade, our understanding of rationality cannot be limited to one aspect or the other.

Consequently, three important points are raised. The first is that the use of cognitive heuristics in the domain of interstate relations need not be framed as a failure of rationality. Despite recent findings in cognitive psychology, scholars in international relations and political science continue to frame cognitive heuristics as low-cost strategies that result in sub-optimal decisions. This paper instead has highlighted the importance of fitting strategies to the appropriate environment, as even complex approaches can result in poor outcomes if used incorrectly.

Second, despite the performance of heuristics in evaluating coercive outcomes in cyberspace, these results are not generalizable across all forms of cyber interactions. While it does appear that heuristics perform better when explaining cyber coercion, it does so because environmental structures are efficiently (and correctly) exploited by underlying cognitive processes. These conditions, however, may not exist in cases of disruptive cyber operations that form much of the interactions in cyberspace. For these, the environment of uncertainty gives way to one of risk due to the well-documented effects of the tools and tactics employed. This consequently enables the use of normative strategies that can better exploit the available information.

Third, decisions in the face of crisis cannot be assumed to emerge from the thoughts of a single individual; unique organizational dynamics contribute to the nature of the decisions made. Furthermore, other factors, such as audience costs that are not addressed in this paper, may also be significant with respect to responding to coercion. This is worth noting given the salience of issues that color various interactions in cyberspace.

The field of cyber security is still in its infancy. Yet with threats evolving both in terms of complexity and scope, there is urgency for academics and policy makers alike to understand state behavior in response to events within cyberspace. This paper contributes to this endeavor by offering an avenue of analysis that has rarely been considered by those in the field but whose insight can assist in maintaining stability within this virtual domain.

Developing Organizational Capabilities to Manage Cyber Crises

Gabi Siboni and Hadas Klein

The increasing number and complexity of cybersecurity incidents have led many organizations to develop procedures and capabilities to manage them. These include real-time response capabilities, technological capabilities, and the formation of teams charged with maintaining organizational information systems. These efforts are liable to be insufficient, however, because they sometimes fail to consider managerial aspects and the skills and tools required of the technological teams to manage crises while trying to confront a cyber incident. This might result in the situation rapidly spiraling out of control, thus becoming a severe crisis with financial, legal, and reputational ramifications, which affect the assets of the entire organization. This essay analyzes the way to develop capabilities to allow organizations to effectively manage crises in information, telecommunications, and cyber.

Keywords: Cyber, cyber crisis, cybersecurity, recovery, crisis management, business continuity

Introduction

In May 2017, British Airways experienced a severe crisis. According to the company, a mishap at the server farm, caused by an electrical surge that stemmed from turning the system on and off, paralyzed the company's ability to operate its flights for several hours. Consequently, many flights were

Dr. Gabi Siboni is the head of the Cyber Security Program at the Institute for National Security Studies. Hadas Klein is a research associate with the Cyber Security research program at the Institute for National Security Studies.

cancelled, and more than 75,000 passengers were stranded. The damage to British Airways became even worse because the various professionals had failed to understand and fix the actual error so as to minimize the effects on the company and its customers.[1] As a result, the harm to the company, in terms of the bottom line and its reputation, was and remains vast.

This incident was a reminder of the tremendous importance of setting up and drilling a crisis management system in companies that rely upon computer infrastructures in order to function. At present, most managers understand that cyberattacks are inevitable. No matter how professional the organization's cyber defense team, it is highly probable that, sooner or later, the organization will find itself under a cyberattack and attempts will be made to breach its computer systems and/or damage them. Therefore, companies and organizations are investing a great deal in proactive defensive capabilities designed to identify attacks in the early stage before they become full blown and cause real damage. Furthermore, organizations are also investing in new approaches and tools, such as cyber intelligence, continuous network monitoring, and tools detecting anomalous behavior. However, despite all means of defense, organizations must continue to ensure they have the capabilities to handles crises stemming from severe cyberattacks.

In recent years, several cyber crises besetting different sectors developed into significant events, sometimes because of failures in crisis management. Cyber crises of this kind can easily damage customer trust and the company's revenues, reputation, and more. Cyber crises can also threaten managers personally and lead to their resignations or dismissals. An example of a failure in crisis management because of improper preparation was experienced by TalkTalk, the British communications provider, in October 2015. TalkTalk managed the crisis in a confused, opaque, and inconsistent manner, leading to the conclusion that the company did not have any clear crisis management plan in place.[2] Two days after the attack had been discovered, the company still was unable to isolate the damage, assess its scope, identify the attacker, or even put its finger on the reason for the attack. The crisis cost TalkTalk an estimated £60 million in direct and indirect losses in terms of damage to

1 Nicola Harley, "British Airways IT Crisis Mystery as Energy Suppliers Say There Was No Power Surge," *The Guardian*, May 31, 2017.

2 Lucas Fettes, "What Lessons Can All Organizations Learn from the TalkTalk Security Breach?" November 12, 2015, http://www.lucasfettes.co.uk/what-lessons-can-all-organisations-learn-from-the-talktalk-security-breach.

reputation, loss of customers, and more. About eighteen months after the incident, following an investigation by the British regulatory agencies, the company's CEO was dismissed. The report of the regulatory agencies clearly stated that the CEO was responsible for the company's lack of preparedness to manage a cyber crisis.

Unlike TalkTalk, the US infrastructure company Dyn, which in October 2016 experienced one of the worst denial-of-service attacks to date, succeeded within a few hours to repel the attack and prevent an escalation to the point of crisis. Company employees said that they constantly had drilled and prepared for such scenarios, and that the drilling focused not only on technological aspects but also on articulating situation assessments, making decisions under pressure, and communicating with management.[3]

Building organizational capabilities to handle a computer and cyber crisis is a crucial component in the overall construction of every organization's defensive and business continuity capabilities. This essay analyzes the theoretical background of crisis management and suggests examining the development of four basic components that allow an organization to successfully face computer and cyber crises: creating an organizational concept for dealing with a computer and cyber crisis; cultivating the human factor and organizing the personnel into a crisis management team; acquiring or developing technological tools and organizational processes that can help realize the organizational concept; and assimilating all this through drills, exercises, and simulations.

Clausewitz famously noted that "war is the realm of uncertainty."[4] This is also true for crises in cyberspace because the uncertainty—the "fog of war" —and the difficulty in formulating a situation assessment hamper making decisions and implementing actions that can resolve the crisis and generate a quick recovery. Developing these capabilities will undoubtedly lead to more effective handling and managing of any crisis as well as better outcomes for the organization.

---

3 Christopher Roach, "Lessons Learned from the Dyn Attack," *CFO.com*, February 9, 2017, http://ww2.cfo.com/cyber-security-technology/2017/02/lessons-learned-dyn-attack.

4 Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret, vol. 1 (Princeton: Princeton University Press, 1976), p. 101.

Theoretical Background: Crisis Management Strategy

In cyberspace, like elsewhere, there is no single definition of "crisis" and no single criterion for applying the term; often, the concept is overused. Not every cyber incident in an organization necessarily leads to a functional crisis requiring special attention; most cyber incidents are managed by routine processes, such as handling malware infections, repelling weak denial-of-service attacks, and so forth. Usually, such incidents do not damage the organization in the short and long term, and cyber security and information security teams manage them as a routine part of their job. Severe cyberattacks, however, can cause lasting damage to an organization's ability to function and provide service to its clients and customers. These cases are indeed crises requiring special attention.

Olga Kulikova and her colleagues have analyzed the purpose of exposing a cyber crisis in an organization.[5] They claim that such exposure entails four important aspects: First, it improves protection and the ability to articulate a situation assessment; second, the exposure will help the company meet regulatory demands and standards; third, the exposure might damage the organization's financial resilience; and fourth, the organization's reputation might suffer as a result of a crisis, which in turn could affect the business results of the organization.

One model analyzing the process of managing a crisis is the bow-tie model developed in 1979.[6] It positions the incident at the center and characterizes the defenses and controls designed to prevent it, as well as the steps that must be taken to minimize the damage once the incident occurs. Diagram 1 below illustrates this model in the context of a cyber incident:

5 Olga Kulikova, Ronald Heil, Jan van den Berg, and Wolter Pieters, "Cyber Crisis Management: A Decision-Support Framework for Disclosing Security Incident Information," *International Conference on Cyber Security (CyberSecurity) 2012* (2012): 103–112, https://doi.org/10.1109/CyberSecurity.2012.20.

6 Steve Lewis and Kris Smith, "Lessons Learned from Real World Application of the Bow-tie Method," (paper presented at the American Institute of Chemical Engineers, Sixth Global Congress on Process Safety, San Antonio, Texas, March 22–24, 2010).

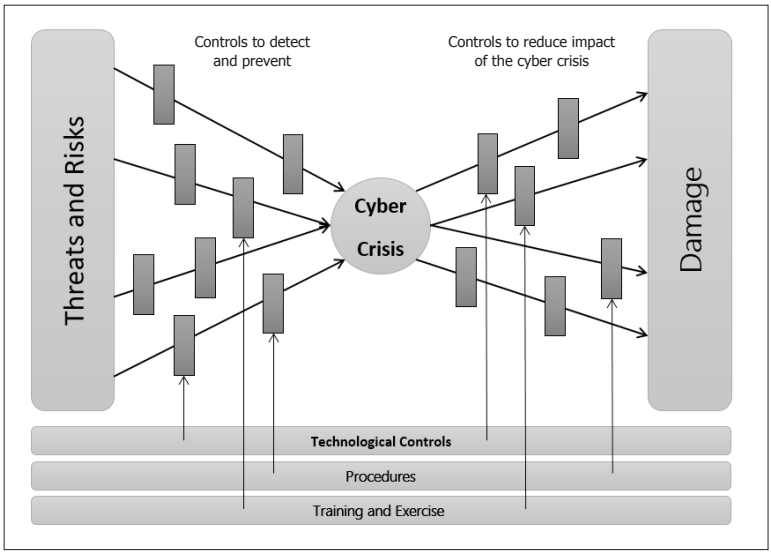

Diagram 1: Bow-Tie Model in the Context of a Cyber Incident

The process of managing cyber crises requires building capabilities that will make it possible to formulate situational awareness throughout the crisis. This process requires constant tracking of a crisis' developing parameters. "Situational awareness" is a term used during crisis management to describe the best possible assessment of what is taking place at any given moment, the possible ramifications of this crisis, the degree of uncertainty of the assessment, the organization's ability to contain the crisis, the way the crisis could develop and further deteriorate, and what could occur later. Situational awareness also describes the organization's active and available defenses against threats. Situational awareness is the foundation for a situation assessment, which is needed to make operational decisions, prioritize events, and handle them based on their threat/risk level and their inherent potential for damage.

The importance of the process of constructing situational awareness is described by Ali Rashidi and his colleagues[7] who analyze the process during a cyber incident as a critical component in the ability to make informed

7 Ali J. Rashidi, Kourosh D. Ahmadi, and Mostafa Heidarpour, "Cyber Situational Awareness Using Intelligent Information Fusion Engine (IIFE)," *Cumhuriyet Science Journal (CSJ)* (Cumhuriyet University Faculty of Science) 36, no. 3 (2015): 3218–3229.

decisions. The authors suggest a model for information fusion to allow a continuous process of providing updates while relying on expert systems.

Barford and his colleagues analyze the phases of the process of building situational awareness.[8] The first phase requires an understanding of what is happening at that moment. This phase is activated after initially categorizing the warnings received and analyzing existing data. The process continues with the goal of understanding the meaning of the incident and the extent of its impact on the organization's critical processes. At the next phase, the authors suggest to comprehend the process of development of the incident and finally to understand how it happened. All these phases are preliminary to the process of making a situation assessment, the purpose of which is to determine the actions to take in order to contain the incident and minimize its damage.

The dimension of time adds further complexity. Often, it is difficult to define the transition from a low-intensity cyber incident, which only requires the routine intervention of the technological team to ensure it remains localized, to a high-intensity cyber incident, which develops into a crisis that has significant ramifications for the entire organization and requires the intervention of non-routine and additional capabilities. One may describe the transition point from a routine cyber incident to a cyber crisis as follows: At first, a hidden gap is created between how the computer systems are functioning and how they are supposed to function according to the organization's service definitions. At this phase, routine intervention is applied. If the situation deteriorates and the gap widens and accelerates and could spread to other areas, more extensive and in-depth efforts are needed.

The Bank of Israel's Directive 361 defines several phases in handling a cyber incident:[9] the detection phase, when there is an initial investigation of the cyber incident; the analysis phase, which refers to a comprehensive and in-depth investigation of the cyber incident in order to determine the possible avenues of action to stop the attack; the containment phase, which is designed to gain initial control of the incident in order to stop the crisis and prevent further deterioration; the eradication phase, designed to neutralize the

8 Paul Barford et al., "Cyber SA: Situational Awareness for Cyber Defense," *Cyber Situational Awareness*, ed. Sushil Jajodia, Peng, Liu, Vipin Swarup, and Cliff Wang (Boston: Springer US, 2010).

9 The Supervisor of Banks, Directive 361, Proper Bank Procedure [1] (3/15), *Cyber Defense Management*, March 2015 [in Hebrew].

event in order to minimize the damage as much as possible; and the recovery phase, during which the organization returns to full and proper functionality.

The capabilities required to manage a crisis can be characterized according to its chronological phases. The first is the preliminary phase of the routine, during which an organization should carry out actions to reduce the probability that a crisis could develop and increase preparedness for managing a crisis, should one occur. In his book *Crisis Management Strategy: Competition and Change in Modern Enterprises,* Simon Booth lists several parameters affecting an organization's ability to manage a crisis, which, he says, must be developed beforehand. The first is planning. At the preliminary phase, organizations should invest resources in planning how to face a crisis.[10] Once an organization finds itself in a crisis, it transitions to the second phase—managing the actual crisis—in which the organization needs a variety of different capabilities to confront the crisis and minimize its damage. The third phase is the post-crisis recovery, which includes an investigation of the incident and drawing conclusions and learning the lessons of the crisis. These phases presented along an axis of time are shown in the following chart:

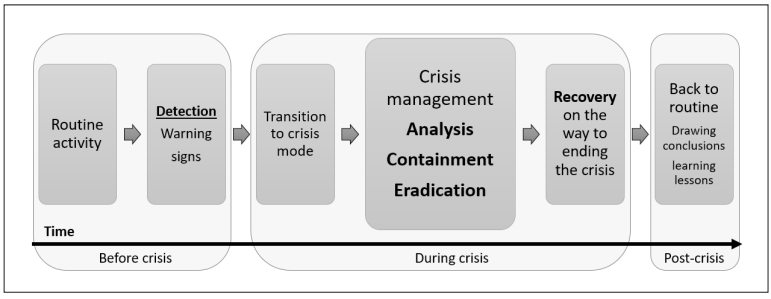

Diagram 2: Chronological Phases of Managing a Crisis

Developing an Approach to Crisis Management

The first milestone is developing an organizational approach to crisis management. Such an approach must include several basic components, the first which relates to determining measures for reasonable downtime and the levels of functioning required for all the computerized systems of the organization. This process requires the organization to rely on an analysis of

10 Simon A. Booth, *Crisis Management Strategy: Competition and Change in Modern Enterprises* (London, New York: Routledge, 1993), p. 13.

its computerized systems and their degree of criticality to the organization's overall functioning. This analysis, called the business impact analysis (BIA), is one component in building a business continuity plan. By using this tool, it is possible to analyze and determine the scope of functioning of each system and the time needed restore it to full operational mode. Such an arrangement reflects the resources for managing the organization's crisis, because an organization that can afford to suspend contact with customers for a few hours differs radically from a bank that suspends its online service or an airline forced to cancel flights, which is liable to cause financial losses and damage to its reputation

The development of such an approach is needed also for the sake of defining what constitutes a crisis and in creating a common language and clear rules for managing it. Determining that a crisis is underway and assessing its severity have immediate ramifications on the resources the organization should allocate to manage it. These resources should relate to the scope of the team managing the crisis, the skills and expertise of the team members, the technological and other means required for the team to operate, and lastly, the extent of training and drilling that the team undergoes. After defining crisis situations, the approach needs to determine the working processes of the organization in its usual, pre-crisis routine and during the crisis itself, and finally determine the post-crisis investigation and learning processes. Furthermore, the approach should determine the responsibility of office holders in the organization during crisis situations.

The development of the approach and the complexity of cyber crises and organizational crises in general require the input of many factors in the organization in addition to the teams providing the technological response to computerized and communications services. Their involvement requires coordination and management of several disciplines, including the management of the legal ramifications related to the operation and safekeeping of databases; management of the regulatory obligations that go into effect the moment a crisis is declared; management of the damage to the organization's reputation; the involvement of the risk management personnel and those in charge of cyber defense in law enforcement agencies, and more. Therefore, as part of preparing for a cyber crisis, it is critical to establish an organizational cyber crisis management committee, which includes the organization's senior

managerial team, such as the chief executive officer, the chief financial officer, the legal counsel, and the director of public relations.

The obvious advantages of including senior management in the cyber crisis management committee are the ability and authority to operate at two complementary levels: The committee should routinely examine regulatory and legal aspects in various crisis scenarios and define financial aspects related to crisis management; validate escalation plans up the managerial chain and contingency plans for managing various media and communications channels when crisis strikes; and during a crisis, the committee should help balance what takes place within the organization and outside of it in order to maintain its reputation and minimize any legal obligations that might occur during the crisis, while maintaining objectivity and ensuring processes of prioritization.

Developing Manpower and Organizing Personnel in a Crisis Management Team

One of the advantages of training an intra-organizational team to handle crises is the ability of such a team to optimally analyze the array of possibilities and courses of action. It is safe to assume that no external party—no matter how experienced—knows the organization as well as the professional teams, business process managers, and senior management. Moreover, intra-organizational team members usually have professional authority and are recognized as such, a factor that can facilitate their work when they must manage a crisis.

To take advantage of the organization's internal resources and realize the organizational approach, it is necessary to train personnel. The process of selecting the various personnel requires a clear definition of the range of functions, the responsibility of the crisis management team, and its interface with stakeholders within the organization and outside of it. It is also necessary to define the skillsets required of these professionals as well as the knowledge and experience they must possess. At the next phase, it is necessary to define the managerial skill and expertise that a member of a crisis management team must have to be able to do his or her job. Such a definition must answer the question: "What skills and expertise are needed to manage a crisis effectively and what does a team member need in order to act effectively?" At the third phase, it is necessary to define the knowledge

and experience required of all members of a crisis management team. Each one should be intimately familiar with the business environment—not just the technological environment—and should therefore be familiar with the organization's business activities, at least at a level of basic understanding. This knowledge can provide team members with the ability to prioritize the management of the crisis based on understanding the criticality of the business processes that have been damaged.

The organization's technological team will face a range of challenges during a cyber crisis, including formulating an up-to-date situational awareness, usually on the basis of partial information, and an optimal response in order to recover rapidly and return to reasonable functioning. When a cyber crisis generates immense public pressure, the organization's managers must provide answers to customers and other stakeholders, further increasing the pressure to which the professional parties are subjected.

The technical cyber crisis management team is the body charged with handling the technological aspects of the crisis. It is also the body that directs the professional parties how to deal with the crisis in a way that will reduce damage and harm to the organization's reputation. Ideally, the technical team is also able to leverage the crisis to the organization's benefit. The team's tasks also include making an initial damage assessment, conveying the current situation and its business ramifications, formulating an action plan for the business processes managers and management, declaring an emergency situation, and managing the incident. These are complex tasks that go beyond comprehending the technological aspects and the organization's computerized and communications systems; rather they demand also a broader understanding of the business, legal, and PR-related effects of a cyber crisis.

When facing a crisis, the crisis management team is subjected to a great deal of pressure, which might impede its functioning. The feeling of pressure intensifies as the gap grows larger between the means and skills needed to confront the crisis and the ability and resources available to the team in practice. It is possible to characterize two types of skills the team should possess: professional/technological skills that involve an intimate familiarity with the organization's technological and managerial systems and soft skills that concern the development of personal and group abilities helpful in the crisis management process.

Developing the professional/technological skills is a process requiring training and professionalization in a range of the organization's technological systems, including the infrastructures and communications systems, the data servers, and the end applications. This should be accompanied by a profound understanding of the management structure, including decision-making processes, the structure of authority and sources of knowledge, as well as all the critical systems and processes at a level that will allow for an analysis of the incident and a mapping of the entities relevant to handling it. To improve the business and organizational understanding of the crisis management team, we recommend brief meetings with the managers of the organization's critical business processes so that the team can come to appreciate the complexity, importance, and challenges inherent in those processes.

The head of the crisis management team should be a member of the organization's management, and it is critical that he or she possess thorough and precise knowledge of the technological aspects and their impact on business processes. Hays and Omodei have determined that the head of a crisis management team should possess a certain combination of personal and interpersonal qualities, including a high tolerance for pressure, self-awareness, and mindfulness of every member of the team, in addition to good communication skills.[11]

A crisis management team should include a member charged with all aspects of coordinating the crisis with the business units. This team member must have a good knowledge of the organizational structure and the administrative aspects required for organizational functioning. The team should also include technological personnel who possess cumulative knowledge of the organization's infrastructures, communications, servers, applications, and databases. When a crisis affects several of the organization's sites, it is important to station representatives of the crisis management team at every site affected, while ultimate coordination must be centralized.

As noted above, the personal characteristics of the crisis management team should also include soft skills, such as interpersonal communications, the ability to listen, emotional intelligence, persuasiveness, creativity,

11 Peter A. Hays and Mary M. Omodei, "Managing Emergencies: Key Competencies for Incident Management Teams," *Australian and New Zealand Journal of Organizational Psychology* 4 (February 2012): 1–10.

precision, problem solving, team work, the ability to make decisions under pressure, and more. These can be developed and improved and eventually implemented during the crisis management process.

Technology

Many tools can help manage cyber incidents. As part of its approach, the organization must decide, depending on its needs, whether to use off-the-shelf tools or develop custom-made ones. Technological tools are extremely important in supporting an organization's crisis management process. They should provide a response in its many stages, such as formulating a current understanding of the situation and carrying out a situation assessment, supplying a supportive system for crisis management—including the ability to preserve and retrieve information from databases from previous incidents, whether they occurred within the organization or in other settings—and the ability to document for the sake of drawing conclusions for the future. The crisis management system allows for mechanical surveillance of the various procedures and processes and emphasizes the priorities in managing the incident by means of previously entered scenarios based on critical business processes. The system also enhances intra-team and intra-organizational communications during an event.

Overall, a crisis management tool is meant to respond to several fundamental needs:

- To create an operational log that is organized as a table and breaks down the process of the crisis. Use of the operational log enables the team to document the cyber incident from the moment it happens and reflect upon it as it occurs. The log's purpose is to help understand the situation, support decision-making processes, and investigate once the crisis ends. The log must include the exact times of the incidents, descriptions of testimonies, facts, and operating assumptions.
- To serve as a platform for communication among key personnel in the organization and stakeholders during the crisis. Rarely do key personnel find themselves all together in the crisis management room; therefore, it is necessary to provide them with a tool that allows them to communicate and understand the developing situation from any location at any time.

- To create one central virtual space for concentrating all the information about the cyber incidents. Creating such a space ensures that the technological teams and the decision makers are operating on the basis of the same facts.
- To help understand the unfolding situation using a range of different cause-and-effect interpretations that are characteristic of the world of information systems, while handling the full volume of cyber incidents and their rapid rate of development.
- To help reduce pressure to allow for objective decision making and a structured use of processes whereby the handling of the crisis is passed up the management chain.
- To support communication based on the organization's matrix of communication and escalation. Crisis management systems make it possible to feed in advance the communications matrix and automatically send updates when previously defined conditions are realized.
- To help understand the significance of events so that the bits and pieces of information gathered from different sources are pulled together to create a full picture, all while assessing the quality of the information, and sorting and organizing it in a way that makes it easily retrievable later.
- To support the process of formulating a possible course of action on the basis of known data while interpreting and analyzing the relevant facts in order to understand how the situation may develop.
- To examine the analysis of the situation and its ramifications given the actions taken. At this stage, a new phase begins, namely that of formulating an updated understanding and assessment of the situation, based on the changes that have occurred due to the actions taken and new data from outside the organization.

The use of technological tools that can help the above-described processes significantly will enhance the efficiency of the work of the crisis management team. Diagram 3 below is a schematic representation of the process that the technological systems must be able to support:

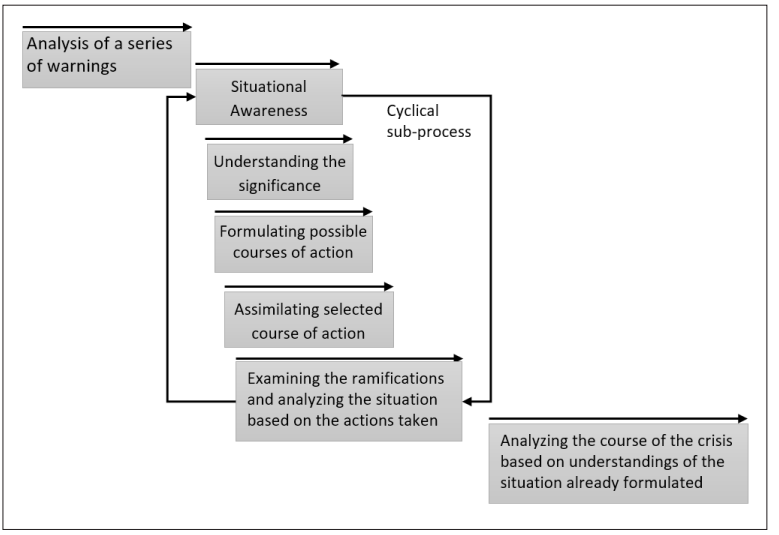

Diagram 3: Representation of the Processes that the Technological Systems Should Support

Another group of technological tools relates to learning from previous cyber incidents both inside and outside the organization. During a crisis, the crisis management team cannot be expected to analyze in-depth why the incident occurred. Such analyses must be carried out in an investigation following the cyber incident as part of the organization's efforts to draw conclusions and learn from the crisis. During the crisis, the focus should be on stopping and eradicating the incident and rapidly recovering the organization's systems to their pre-crisis functioning while setting clear priorities. Sometimes, a temporary fix is needed; at other times, using means that bypass the problem until it is resolved is the right thing to do.

An important tool in diagnosing a crisis is a database of all historical cyber incidents and crises in the organization, a similar index describing cyber incidents in the organization's business sector, with as much detail as possible, as well as those that have occurred in the organization's geopolitical environment. For example, a bank would be wise to maintain a listing of all extreme cyber incidents that have taken place in other banks all over the world. This tool allows the crisis management team at the bank to identify familiar problems and errors caused by similar incidents in the past, thereby gaining information on ways to bypass the problems when they are identified.

This is an automated, structured tool that must include a smart data retrieval engine, including data written in free text format.

Crisis management tools should also document the crisis and the work processes as it occurs so that it can be input into the organizational learning system and used during the current crisis and future ones. The documentation should include the development of events, a description of the warnings issued and their reporting, and the decisions made at every stage. This documentation is significant in various ways should a similar scenario develop in the future or in case the crisis is not yet over despite the steps taken, including the formulation of a current understanding and a situation assessment. In addition, a summary report should be prepared and distributed to all internal stakeholders—including the management and other relevant parties—and to external stakeholders, as per the relevant regulatory directives.

Assimilation: Training, Practice, and Drills

Improving abilities and attaining a high level of preparedness are largely based on training, exercises, and drills as being an integral, structured part of the process of realizing the organization's approach to crisis management. Several components of the assimilation process are involved.

The crisis management team usually includes employees with extensive training and knowledge in computerized systems and the organizational cyberspace. Their role in the team is in addition to their routine jobs. Nonetheless, before becoming a member, all candidates for the crisis management team should undergo some basic training, which should cover the organization's crisis management rules and principles, crisis plans and procedures, and understanding both the business environment and the organization's technological tools for crisis management. The training should also include aspects of identification, documentation, classification, and prioritization; initial diagnosis of the crisis; investigating its development; means of communications and escalation (i.e., passing the handling up the management chain); the organization's existing sources of information and information gathering; and finally, ways of concluding a crisis, investigating it, and learning lessons from it.

In addition to this basic training, exercises should routinely be carried out, including so-called "tabletop exercises" and crisis management team drills under conditions as real as possible, as well as large-scope exercises

that also incorporate the organization's management. The purpose of tabletop exercises is to analyze relevant reference scenarios in the absence of the regular work environment's pressure. Such exercises greatly add to the crisis management team's knowledge, expand the team members' common language, and increase cooperation among them. In these exercises, it is possible to encourage team-thinking processes and focus the team members on dealing with a range of scenarios and controlling the directions in which they develop, while expanding internal and external communications and interactions with stakeholders and improving the mutual understanding of team members' responsibility and authority. Such exercises also make it possible to validate the organization's policy and procedures.[12] It is best if they include professional guidance[13] aimed at increasing the motivation and willingness of the team members to participate in the exercise and allow them to succeed.[14] The set of exercises encourages the crisis management team to consider failed patterns, such as thinking in terms of concealing or minimizing the crisis or giving an immediate solution in order to extinguish the fire.

In addition to tabletop exercises, it is necessary to hold broader-scoped exercises and drills simulating reality as closely as possible. Several principles should be realized while holding them:

- **Formulating the scenario's nature:** Formulating scenarios of glitches, crashes, and other acute problems in the organization's critical systems, while relying on an analysis of the business continuity plan and the business impact analysis. Doing so ensures the handling of the operational core of the organization's cyberspace. We recommend that exercise scenarios be formulated in a way that the crisis management team is exposed to scenarios of increasing complexity.
- **Creating a technological environment:** Constructing a technological environment for the exercise scenario makes it possible to simulate

12 Brent D. Ruben, "Simulations, Games and Experience-Based Learning," *Simulation & Gaming* 30, no. 4 (1999): 498–505.

13 Tim Urdan, "Intrinsic Motivation, Extrinsic Rewards and Divergent Views of Reality," review of *Intrinsic and Extrinsic Motivation: The Search for Optimal Motivation and Performance*, ed. Carol Sansone and Judith Harackiewicz, *Educational Psychology Review* 15, no. 3 (September 2003): 311–325.

14 A. J. Faria and W. J. Wellington, "A Survey of Simulation Game Users, Former Users and Never Users," *Simulation & Gaming* 35, no. 2 (June 2004): 178–207.

reality as closely as possible, while minimizing the exercise's effect on the organization's operational functioning. The technological environment for the exercise must allow communication, event streaming, and the establishment of an environment of sensors for the computerized systems and technological infrastructures.

- **Constructing the scenario:** The exercise should be constructed on the basis of events that reach the crisis management team from the operational systems and their operators. The crisis management team must try to identify the source of the incident by examining the events and the technological sensors at its disposal (e.g., an overload on computing resources, a glitch in copying data or log files, and so forth). The scenario must include the backstory and events streamed during the exercise, some of which are simply noise unrelated to the incident directly.
- **Adjusting the exercise:** The crisis management team and the supporting system of management must identify the source of the problem in the computer systems and the essence of the cyber incident they are supposed to handle. To make this possible, it is necessary to prepare a bank of events to be streamed, based on the development of the handling of the scenario, in order to maximize benefit from the exercise and ensure optimal training for all involved.
- **Controlling and mentoring:** It is critical to maintain a control system in tandem with the exercises. As an exercise unfolds, this system can note the strengths and weaknesses of each team member and of the team and thus focus the learning process and enhance the professional development of both members and the group. During an exercise, it is important to calibrate basic existing capabilities and use the data gathered in order to set measures for necessary improvements and the success of future exercises. The results of the exercise make it possible to focus the program of professional seminars and training for the members of the team.

In addition to the training of the technological team and as part of the process of preparing to handle a crisis, it is also important to hold exercises for the organization's management. This is critical for building a common language, understanding the constraints in sharing information with external stakeholders during a crisis, and giving the technological team peace of mind and the space it needs to handle a crisis without management pressure. Such pressure does not help, and in most cases, it only gets in the way.

Conclusion

The growing number of cyber incidents and crises has greatly increased the need of organizations to develop their capabilities to handle them. Proper handling of a cyber crisis can reduce damage and lead the organization to rapid recovery, while failure to handle a crisis is liable to lead the organization to its collapse.

Cyber event management is an organizational task involving many of the organization's employees, from the cyber and information security personnel to the members of the board of directors. How the organization handles an incident has just as much impact as the technological capabilities the organization has at its disposal. Including a cyber crisis management policy reflecting the organization's needs and goals as part of the organization's overall cyber strategy is vitally important.

An organization's ability to handle a crisis largely depends also on its ability to improvise and function under pressure. These abilities are commonly attributed to Israel's management culture, but they are far from sufficient in the complex reality and chaos generated in a cyber crisis and in which a crisis management team is supposed to function. It is therefore wise to rely on orderly methodologies of cyber and computer crisis management and on a qualified array of personnel that has trained for such an event in its day-to-day work. As such, we recommend that organizations formulate a plan to develop tools and skills as described in this essay and set up an orderly program for training, simulations, and drills.

Turkey—Challenges to the Struggle against Cyber Threats

Ofir Eitan

Turkey is one of the most technologically, economically, and institutionally developed countries in the Middle East. At the same time, it is one of the countries most exposed to cyber threats. The Turkish government has taken steps in recent years to narrow the existing gaps in defense against cyber threats, but its efforts in this area have not yet produced the desired results. This article analyzes Turkey's national cyber defense deployment and cites a number of structural challenges resulting from long-standing Turkish policy. The Turkish government will have to find solutions to these challenges in order to achieve the goals of its national cyber defense programs.

Keywords: Cyber, Turkey, policy, national security, political economy

Introduction

Cyber threats have had a growing influence on our lives in recent years and thereby on policies of many governments. Many countries accordingly have begun taking steps for devising a national strategy in cyberspace and forming infrastructure to defend against cyberattacks. Since reports of Stuxnet, Flame, and Shamoon in the media and of distributed denial-of-service (DDoS) attacks against the US financial sector, it has appeared that the Middle East has also become an active player in the lively cyberwar theater. The identity of the attackers in cyberspace is an ambiguous question, but the United States,

Ofir Eitan is a certified information and cyber security manager and a cyber threat intelligence officer with the rank of major in the IDF reserves. He has a BA and an MA in the history of the Middle East from Tel Aviv University.

Israel, Iran, and other countries in the Persian Gulf have nevertheless been mentioned in this context in recent years.

Turkey is one of the most developed countries in the Middle East, a regional power, and an important member of NATO; nevertheless, there is a major deficiency in the capabilities of its institutions to cope with cyberattacks. For example, only in 2016 was a national center established for coordination and cooperation in defense against cyberattacks. Only in July 2017 was the Turkish cabinet presented with a draft bill for strengthening defense of cyberspace in public agencies, by integrating security experts from various disciplines, including white hat hackers, professionals whose job is to improve the level of network computer security through controlled penetration tests and risk assessments. The aim of this measure was to expand the authority of the National Intelligence Coordination Center (NICC), a department subordinate to the Information and Communication Technologies Authority of Turkey (Bilgi Teknolojileri ve İletişim Kurumu [BTK]), which is responsible for handling and responding to cyberattacks throughout the country and for distributing actionable information and helping to protect all public agencies.[1]

Turkey has not yet consolidated a national protective framework in cyberspace incorporating the ruling institutions, security agencies, national infrastructure, and private entities, even though long ago it had formulated a national strategic plan in this matter, the 2016–2019 National Cyber Security Strategy and Action Plan.[2] The Turkish plan resembles similar processes that have developed in other countries in the western world, while considering the specific situation in Turkey, which must cope with diverse and constant cyber threats to the country's infrastructure.

Beyond the bureaucratic barriers, Turkey faces structural challenges that obstruct the steps necessary for the growth of high-level local infrastructure in the cyberspace. The internet and data communications sector, which is one of the industries that is knowledge-intensive, has unique characteristics that differ from those of other industrial sectors. As a result, the sphere of cyber warfare—the world of virtual attacks on computer systems and the

1 Şeyma Nazli Gürbuz, "Turkey Adopts Cybersecurity Strategy, Fights Cyberterrorism," *Daily Sabah*, August 10, 2017, https://www.dailysabah.com/war-on-terror/2017/08/11/turkey-adopts-cybersecurity-strategy-fights-cyberterrorism.

2 Merve Seren, "Turkey Steps up Counter-Cyber Attack Efforts," *New Turkey*, January 24, 2017, https://thenewturkey.org/turkey-steps-up-counter-cyber-attack-efforts/.

defenses against those attacks—requires a special allocation of resources, particularly for the development of human capital.

Given these basic insights, I argue that Turkey's long-term centralized policy is responsible for the fundamental challenges that the country faces today in dealing with cyber threats to its national infrastructure. These challenges can be separated into two spheres that greatly affect Turkey's ability to develop its power in cyberspace: the policy and bureaucratic challenge and the organizational culture.

The analysis begins with a brief description of the state of Turkish national policy in the field of cybersecurity. The above-mentioned two spheres that contain the structural challenges facing Turkish decision makers in developing power in cyberspace are then analyzed. This essay relies upon a number of basic assumptions from the capitalist economic approach for the purpose of theoretically analyzing the development of the challenges facing Turkish policy.

Turkish National Cybersecurity Policy

Studies in recent years have presented data that should keep Turkey's defense leadership and its decisions makers awake at night. For example, as early as 2012, it was reported that Turkey was among the ten most attacked countries in the world in the cyberspace.[3] Some of the world's leading information security and communications companies, such as Trend Micro, Fortinet, and Akamai, reported in 2016–2017 that Turkey headed the list of countries in Europe and worldwide that had been most frequently cyberattacked.[4]

An analysis of the cyber threat landscape shows three main players threatening Turkey's governmental and commercial internet networks: political Kurdish players, the Gülen movement (FETO by the Turkish government), and cybercrime. An example of a Kurdish cyber threat was the widely-reported attack against the website of the Turkish Ministry of Finance, which had been defaced with propaganda corresponding to the agenda of the PKK, the underground Kurdish organization, and caused it to crash.[5] In this

3 Aydin Albayrak, "Turkey among Top 10 Countries Subjected to Cyber Attacks," *Sunday's Zaman*, July 1, 2012.

4 Seren, "Turkey Steps Up Counter-Cyber Attack Efforts."

5 Umit Kurt, "Cyber Security: A Road Map for Turkey," Strategy Research Project (Carlisle, PA: US Army College, 2012), pp. 8–9; Ümit Enginsoy, "Turkey Centralizes Efforts for National Cyber Security," *Hurriyet Daily*, November 21, 2011.

event, the objective behind this "noisy" attack was clear, but the question of the attacker's identity in the cyber world usually remains unsolved. In this context, other famous attacks can be named, which were directed against Turkish government websites, such as those of the Ministry of Finance,[6] the national police and Turkish Airlines.[7] It is reasonable to attribute these attacks and others like them to Kurdish players as well as cyber criminals.

As using computer and communications networks by institutions and companies in Turkey increases, so does the threat to their proper functioning. It is believed that of the approximately 80 million residents of Turkey, the world's twentieth largest population,[8] nearly 43 million use the internet, putting Turkey in nineteenth place worldwide in the use of this communications medium.[9] This means that Turkey ranks alongside the most developed countries in the family of nations in relation to the number of residents and the extent of internet use. At the same time, however, Turkey lags behind in its national effort to defend its networks against cyberattacks, in comparison with the measures taken by other developed countries.

In October 2010, the Turkish army published the "Red Book," which provides a close-up once every few years of Turkey's national defense strategy. This book suggests that from Turkey's perspective, cyberspace is perceived as a non-conventional threat. In 2011, the Turkish National Security Council accordingly ratified a new national strategy that for the first time also included the problem of cyber threats.[10] As mentioned, a national plan for cyber defense strategy in 2016–2019 was also recently published.[11] This strategy has two main goals. The first is Turkey's recognition that cyber defense is an integral element of national security. The second is to bring Turkey up to par in the qualifications needed concerning the administrative

6 Kurt, "Cyber Security: A Road Map for Turkey."

7 Albayrak, "Turkey among Top 10 Countries Subjected to Cyber Attacks."

8 The figure is correct as of 2009, and it likely that the current number of users is even greater. In any case, this does not materially alter the picture.

9 Central Intelligence Agency, *The World Factbook*: *Turkey*, January 7, 2013, https://www.cia.gov/library/publications/the-world-factbook/geos/tu.html.

10 James A. Lewis and Katrina Timlin, *Cybersecurity and Cyberwarfare*: *Preliminary Assessment of National Doctrine and Organization* (Washington DC: Center for Strategic and International Studies, 2011), p. 20.

11 Seren, "Turkey Steps Up Counter-Cyber Attack Efforts."

and technology measures essential for achieving absolute security for all the national assets in the cyber realm.

The Turkish government institutions have de facto developed cybersecurity functions that are the result of an independent initiatives by government entities; indeed, there is no single authority or supreme agency in Turkey that coordinates national cybersecurity. Among the existing agencies are the Turkish national Computer/Cyber Emergency Response Team (TR-CERT),[12] which operates under the Information and Communications Authority, as well as the first Cyber Fusion Center, belonging to the Turkish Ministry of Defense.[13] Although activity in this sphere relies mostly on imported products, the Turkish army and the National Intelligence Organization (MIT) rely on local technological solutions for cyber defense developed and provided by Havelsan, the "government company for software and systems."

Following the staff work conducted in 2010–2011, Turkey devised a plan for establishing a "Cyber Command" in the Turkish army general staff for the purpose of repelling network attacks against the country. The general staff of the Republic of Turkey announced the establishment of this command in 2013.[14] Media reports and the statement of a senior Turkish army officer shed light on the situation behind the scenes of this new command. This agency, which is constructed along the lines of its American counterpart, has the job of monitoring the entire public internet in Turkey in order to provide a defensive framework for state institutions.[15] The Turkish "Cyber Command" is designed to act in cooperation with the Turkish Ministry of Defense, the National Council for Science and Technology Research (TÜBİTAK), and the Middle East Technological University. This command—headed by an officer with the rank of general—relies on a special budget, is independent in

12 CERT—Computer/Cyber Emergency Response Team is a concept first formulated by Carnegie Mellon University that refers to the need to establish national, institutional, or sectoral centers whose job is to assist targeted communities to prepare for cyber threats and how to cope with them.

13 Seren, "Turkey Steps Up Counter-Cyber Attack Efforts."

14 Burak Ege Bekdil, "Cyber Defense 'Indispensable Part' of Turkey's National Security: Senior Official," *Atlantic Council, Defense News*, December 13, 2013, http://www.atlanticcouncil.org/blogs/natosource/cyber-defense-indispensible-part-of-turkey-s-national-security-senior-official.

15 Kurt, "Cyber Security: A Road Map for Turkey," p. 14; Enginsoy, "Turkey Centralizes Efforts for National Cyber Security."

organizational structure, and includes a special cyber defense unit.[16] According to a statement by the Turkish minister of communications and transportation, Turkey's cyber defense program was put into practice in 2013.[17]

Awareness in Turkey of the need for defense of cyberspace and the potential of the threats in this sphere has increased in recent years, as can be seen from the policy plans and various local initiatives by governmental entities, but from a practical standpoint, Turkey's national cyber defense deployment lags significantly behind in comparison with other western countries. Çetin Kaya Koç, a professor of cryptography at the University of California, described well the situation in cyber defense: "Since Turkey did not complete its cyber transformation in its infrastructure yet . . . in case there is an attack on the infrastructure in the future, such as on metro systems or electricity, there are not enough precautionary measures taken to deal with it."[18]

This situation shows that progress in Turkey's cyber security mechanisms requires not only expediting the bureaucratic processes but also relying on two cornerstones of the country's national resources: trained local personnel and a local infrastructure of research and development. At the same time, as already noted at the beginning of this article, Turkey is obliged to meet many other challenges, resulting from the centralized policies of its government since the establishment of the republic; these challenges create barriers and obstacles that delay the consolidation of these two cornerstones.

The Challenges Facing Turkey in Developing Cyber Power

The capitalist approach to political economy holds that a centralized policy constitutes one of the market failures, delaying manufacturing and technological development and the growth of private entrepreneurship. The philosopher and economist Adam Smith argued that a division of labor between all market players leads to professionalism, saves time in the transition between the various stages of production, and motivates people to perfect production processes. In addition, the capitalist approach does not dispute that the state has an important role to play in economic development and stabilization,

16 Lewis and Timlin, *Cybersecurity and Cyberwarfare.*

17 "Turkey's Cyber Defense Plan to be Ready in 2013," *Hurriyet Daily*, March 2, 2012.

18 Gürbuz, "Turkey Adopts Cybersecurity Strategy, Fights Cyberterrorism," *Daily Sabah*, August 10, 2017.

even in the free market era of our time. In this framework, the state exerts an influence through regulation of the labor market, education, professional training, and so forth, while setting economic policy, passing legislation, and creating enforcement measures within the framework of the tension between the market's decentralization and its centralization.[19]

In a liberal market economy, firms solve market failure through reciprocal relations within the free market, contracts (arrangements), and hierarchy (relations between firms). In other words, according to the classic liberal approach, market failures are solved by the dynamic of the "invisible hand" of market forces. In the coordinated market economy typical of Turkey, firms rely less on competition and more on business networks and reciprocal strategic relations ("incomplete contracts"). In practice, even under the dictates of the free market, centralization in the economy is preserved in the hands of the state and a few powerful economic groups.[20]

The Policy and Bureaucratic Challenge

Until the late 1990s, the Turkish government did not adopt any deliberate policy to encourage private entrepreneurship in general, and high-tech industries in particular. This was the result of a policy of many years standing, originating from the time of the transition from the Ottoman Empire to the modern Turkish Republic. Even thought the Turkish Republic inherited a tradition more than a century old of adopting western technology, its foundations were built upon an impoverished country whose economy rested on agriculture and the absence of any institutionalized private-sector infrastructure.[21]

The first Turkish government following the dissolution of the Ottoman Empire aimed for economic and social development but believed that it should consist of heavy industry focused on manufacturing. For this purpose, and as part of its general centralizing policy, the Turkish government founded government-owned and managed companies, while adopting five-year plans based on the Soviet model. In addition to its centralizing policy, which blocked

19 Peter A. Hall and David Soskice, "Varieties of Capitalism," *The Political Economy Reader*: *Markets as Institutions*, ed. Naazneen H. Barma and Steven K. Vogel (Indiana: Routledge, 2007), pp. 292–303, 307–312.

20 Ibid.

21 Arnold Reisman, "Why Has Turkey Spawned so Few High-Tech Startup Firms? Or, Why is Turkey so Dependent on Technologic Innovations Created Outside its Borders?," *SSRN*, May 26, 2006, pp. 1–4, https://ssrn.com/abstract=904780.

any possibility of private entrepreneurship, all Turkish governments have adopted a development policy that does not accommodate demand for local development. As a result, the construction of Turkey's infrastructure has been based completely on imports. The Turkish government signed agreements with foreign corporations for designing, constructing, and operating large-scale ventures, which passed into Turkish hands at the end of the process. This process has persisted until today. This policy culminated in exclusive dependence on external technology and the absence of any need for local entrepreneurship.[22]

The Turkish government also replicated the format of establishing government companies and corporations in the private sector, with the state targets and the way in which they are implemented remaining identical. Up until the late 1990s, government support for the private sector focused on heavy industry with the main purpose being the creation of as many jobs as possible. This policy had additional consequences, two of which are important in this context. The first was the neglect of knowledge-intensive industries, for which trained, educated, and expert personnel is usually needed, in addition to fewer jobs in this sector than in other sectors. The second was the rise of a class of oligarchs. These were the heads and owners of the large corporations—a conglomerate of families—who shaped demands in the Turkish market according to their needs, and whose interests almost completely overlapped with those of the state. These corporations do not usually need engineers and high-tech personnel, and they therefore perpetuate the technological stagnation, the backwardness within the population, and the focus on blue-collar industries.[23]

Even after the opening of the Turkish market in the late 1990s, local entrepreneurs were confronted with a bureaucratic labyrinth that complicated and even thwarted any sign of local entrepreneurship. This is a significant challenge for the high-tech industries in general, especially the cyber and internet sector. From the beginning, a Turkish entrepreneur seeking to establish a startup finds it almost impossible to raise money other than personal or family capital. Most potential credit for initiatives of this type is in the hands of the banks, which pursue a cautious policy because of the frequent crises

22 Ibid.

23 Ibid, pp. 1–4, 9.

in the Turkish capital market over the past thirty years.[24] Statistics show that less than 5 percent of the available bank credit in Turkey is provided to industrial SMEs (Small-Medium size Enterprises). This is rather ironic, given the fact that SMEs account for 99.5 percent of the establishments in the industrial sector, 66.5 percent of employment in the sector, and 34 percent of value added in the sector.[25]

Even when the banks in Turkey decide to provide credit to business entrepreneurship, many of them are incapable of formulating a proper financing plan and of finding the relevant financial resources to pay for it. Furthermore, alternative sources of financing, such as venture capital funds, angel investments, and capital raising through share offerings are underdeveloped in Turkey in comparison to other western countries. In addition, most loans to entrepreneurial firms in the Turkish market are provided by Halk Bank, the Turkish national bank, which is in the process of privatization.[26] This contrasts with the sources of financing for entrepreneurs in western countries, which come from a broad range of financing and aid instruments, including the government itself, foreign investments, growth-encouragement companies, non-governmental organizations, international trade organizations, and so forth.[27] As noted, economic growth levers of this type are underdeveloped in Turkey. This situation poses many challenges and barriers to the high-tech industries in the country, including the cyber industry.[28]

In terms of the bureaucratic processes that a Turkish entrepreneur faces, it is worthwhile quoting the description of this substantial challenge by Dilek Çetindamar, a professor of management at Sabancı University in Istanbul, who said, "Turkey is the 13th most bureaucratic country in the world . . . an entrepreneur needs 172 signatures from various government agencies in order to receive approval to invest . . . in Turkey an entrepreneur spends 20% of his or her time on bureaucratic issues, this rate is 8% in the European Union."[29]

---

24 Ibid, pp. 8–9.

25 "Small and Medium-Sized Enterprises in Turkey: Issues and Policies," *OECD Report* (Paris: OECD Publications, 2004), pp. 2–33.

26 Ibid.

27 Reisman, "Why Has Turkey Spawned so Few High-Tech Startup Firms?," pp. 8–9.

28 "Small and Medium-Sized Enterprises in Turkey."

29 Reisman, "Why Has Turkey Spawned so Few High-Tech Startup Firms?," pp. 8–9.

Another critical aspect in the free market era is the lack of access to information among Turkish startups. According to neo-liberal economic principles, promotion of economic growth requires the opening of most information and knowledge channels. A study by the OECD (Organization for Economic Development and Cooperation) in 2004 of the small and medium-sized enterprises sector found that the Turkish market lacked knowledge-based agents and communications channels for information sharing. The OECD recommended that the Turkish government refrain from conflicts between legislative bodies and law enforcement agencies over conflict of interest in order to facilitate transparency for the benefit of small and medium-sized enterprises.

In 2001, with the start of the national program for implementing the Treaty on European Union (the Maastricht Treaty), Turkey pledged to undertake basic reforms of its local regulation systems according to the accepted international criteria. This process, together with other measures that the Turkish government is trying to advance, is designed to improve bureaucratic processes and the regulatory systems in Turkey, among other things.[30]

The Organizational Culture Challenge

The cyber realm is notable for its human capital, which distinguishes the know-how and specialists in this sector from the other high-tech industries. Among other things, several characteristics or professional traits are necessary for the development, progress, and attainment of an appropriate level of software engineers, communications network specialists, information security experts, as well as hackers. These are not scientific measures but rather an institutional and organizational environment that generates and facilitates the growth of innovative developments and technological solutions. It is difficult to separate this essential element of the cyber sector from the centralizing institutionalized policy typical of Turkey, because according to the liberal approaches to political economy, a centralizing policy creates barriers to the development of firms and individuals in the internet and data communications sectors that are seeking to break through and innovate in their field.

In order to assess the challenges of the organizational culture facing the creation of human capital in Turkey's cyber sector, the focus should be on two fundamental characteristics to this country: the relations between the

30 "Small and Medium-Sized Enterprises in Turkey"

state and the military and its research and development culture. Our basic assumption is that centralization in the Turkish establishment prevents structural processes (market failure) necessary for the growth of the cyber industry in the country.[31]

Many people regard the defense industries as a spur and catalyst for technological developments in many industrial sectors, especially in the knowledge-intensive industries. Taking this basic assumption into account, it would be logical to conclude that Turkey, in which the army constitutes a pillar of the regime and society, should also be a pioneer in the cybersphere, or at least have a high-quality "toolbox." The reality in the Turkish cybersphere, however, is very different. Prof. Arnold Reisman claims that Turkey has not succeeded in channeling its military effort and defense industries into the development of important technologies in the civilian market, which is essential for growth in the cyber industry. In order to prove his claim, Reisman conducted a theoretical comparison between three countries bearing similarities that are tangential to our discussion: Turkey, Israel, and Iran. Since gaining their independence, these three countries have continuously faced significant national security threats to their sovereignty, and all three have experience in absorbing and integrating high-quality weapons featuring sophisticated technology.[32]

Turkey's defense industries currently export independently developed products requiring highly technical professionalism in air and sea warfare, electronic warfare, and command and control systems.[33] However, the reciprocal relations between the Turkish defense industries and the private firms in Turkey (individuals and organizations) in cyberspace have not led to the development of an adequate "toolbox," because the government cyber industries, like every other technological industry in Turkey, are not developed sufficiently for this purpose. Reisman's findings show that Israel has successfully channeled its military developments for the purposes of both helping economic firms in the country and distributing technologies and know-how in the civilian market. In Turkey, on the other hand, such a process is almost totally absent. Like developing countries, Turkey has

31 Hall and Soskice, "Varieties of Capitalism."

32 Reisman, "Why Has Turkey Spawned so Few High-Tech Startup Firms?," pp. 10–15.

33 Ibrahim Sunnetci, "High-Tech in Turkey – Special Report," *Military Technology* 35, no. 3 (2011):107–110.

learned how to manufacture light weapons and ammunition, but it regularly purchases the more sophisticated weapons in its arsenal from other countries (including Israel).[34]

Prof. Reisman presents a theory for understanding this situation. He compares Israel's military and social fabric with that of Turkey, while emphasizing Israel's uniqueness as the "Startup Nation," although Turkey, like Israel, has compulsory military service. Most of the Israeli military's internal organizational research and development processes are based on the people serving in the army, but the uniqueness of Israel is that the dictates of organizational demand cause the military command to allow space for creativity and extensive action, and the organizational culture encourages the growth of bottom-up ideas and initiatives from within the ranks. When this organizational culture is combined with the fact that the Israeli army finds and selects the candidates from the majority of the population that has reached the age of eighteen and that a high proportion of young people serve in the army, fruitful reciprocal relations emerge between the army and civil society.

Indeed, many civilians in Israel after their military service move into the civilian market with a great deal of high-quality know-how and work experience. In this situation, many doors are open to them in order to channel their creativity for the benefit of civilian companies, some of which are headed by veterans of the security system. In Turkey, on the other hand, there is no such tradition nor is there a similar process of reciprocal fertilization between the military and the civilian market. Thus, even when the Turkish defense establishment spots people in the system with good qualifications, they ordinarily use those people if they choose to remain within the framework of the state-owned defense industries, which mostly operate under organizational and bureaucratic constraints and dictates that delay growth.[35]

Despite the above, it can be argued with a great deal of justification that the existence of close army-society relations does not necessarily create an echelon of excellent human capital for the cyber sector. Even though this axis generates development, various countries in the past and the present have reached a pinnacle of achievement even without the need to find a solution

34 Reisman, "Why Has Turkey Spawned so Few High-Tech Startup Firms?," pp. 10–15.

35 Hall and Soskice, "Varieties of Capitalism"; Reisman, "Why Has Turkey Spawned so Few High-Tech Startup Firms?," pp. 5–8.

to security threats. The investments of both the Turkish establishment and the country's private firms in academic or commercial research are extremely meager. To this should be added the fact that the salaries of academic researchers in Turkey are not high, which tends to keep academic quality at a low level. The institutional organizational culture is not fertile ground for development, sharing of ideas, creation of information and knowledge, and so forth, which are all cornerstones for the progress and growth of the cyber industry.[36]

As a rule, neither the Turkish establishment nor Turkish tycoons have done enough over the years to foster research, development, and technological entrepreneurship. It is important to stress that the Turkish oligarchs do direct capital to the public and the market, but most of the contributions and investment funds are channeled into building schools, universities, and museums. Turkey has no institutionalized mechanism for empowering academic researchers through the private market or encouraging technological entrepreneurship wherever it might be. In order to highlight this, the first technological park in Turkey was founded in 1985 by the Technological University in Istanbul and the municipal chamber of commerce. A similar institution was founded in Ankara only in 1991 by the Middle East Technical University. In contrast, Prof. Reisman points out that the Weizmann Institute of Science, an institution established in Israel in order to export academic findings to the commercial market, among other things, began operating as early as the 1950s.[37]

I have seen fit to conclude this discussion with a quote from Prof. Reisman's research: "Although Turkey changed its government in 1923 and undertook major reforms, it did not change its people, who are steeped in tradition. Historically during the Ottoman Empire, educated Turks have been administrators, bureaucrats, and not business-minded[38] nor particularly technically inclined."[39]

---

36 Reisman, "Why Has Turkey Spawned so Few High-Tech Startup Firms?," pp. 5–8, 10–12.

37 Ibid, pp. 12, 15.

38 When Reisman uses the term "business-minded," I assume that he is referring to business thinking and entrepreneurship in the free market.

39 Reisman, "Why Has Turkey Spawned so Few High-Tech Startup Firms?," pp. 8–9.

Conclusion

Perusal of various Turkish sources in English shows that the academic discussion of the cyber question in Turkey still has not yet reached maturity. Even though quite a few news and media reports of cyberattacks experienced by Turkey can be found on the internet, it is clear that its discussion usually consists of opinion pieces written by various parties. In considering the main processes that Turkey has experienced in the cyber realm, I chose to focus on the challenges facing it, especially the lack of local human capital, which I believe is the core problem. I relied on an analysis of the situation, especially using the findings and conclusions of Prof. Arnold Reisman, together with the use the findings of the 2004 OECD report, which focused on research on the Turkish economy and on making of recommended course of actions for its development. Even though the academic discussion and the analysis I have set forth in these pages are incomplete, they indicate the need to gain a deeper understanding of the fundamentals of Turkish culture in order to decipher the basis for the challenges facing the development of the local cyber industry.

The distinction I proposed between the effect of the centralized Turkish policy on the political-bureaucratic challenge on the one hand and the organizational culture challenge on the other is a purely artificial distinction for the purpose of clarifying the logical argument. In practice, what is involved is a symbiotic relationship between the culture of Turkish society and its government's policy. The current socioeconomic situation in the country shows that a large percentage of the Turkish populations lives in a rural environment and maintains a traditional patriarchal Islamic society. This affects the policy and functioning of the Turkish governments.

The statement by Prof. Dilek Çetindamar describes the situation well: ". . . but rather that 'university graduates' career plans involve working in large companies, since starting up a firm is considered a big risk. Therefore, no tradition of entrepreneurship exists."[40] This statement expresses the main conclusion of this article: In order to foster high-level human capital in the Turkish cyber community, a suitable environment is needed; that is, an infrastructure that encourages initiative and innovation. It appears, however, that Turkey is not an "incubator" that encourages private entrepreneurship, which, according to the accepted formula, is a necessary condition for

40 Ibid, p. 14.

fostering pioneering high-tech personnel and engineers. Furthermore, when Turkey needs special technological solutions, it is likely to choose to import outside knowledge, and each one of the players in the triangle of the state, oligarchs, and society will prefer to channel human capital into the large manufacturing companies, while space for originality and entrepreneurship essential to the cyber realm will remain limited.

Germany's Cyber Strategy—Government and Military Preparations for Facing Cyber Threats

Omree Wechsler

Germany is a leading member of the European Union and one of the world's strongest economies. Consequently, it is a central target for cyberattacks from states, terror organizations, and criminal groups. Dealing with the threat to German democracy posed by campaigns to disseminate false information—plus the cyber threat posed by Russia—has led to changes in the German security concept, causing the German government to seek to increase its cyber independence and to establish offensive capabilities in this space. Understanding how Germany copes with cyber threats and its future plans on this issue is vital for learning and comparing, while it also provides new insights about this problem, particularly for other democratic countries.

The first part of this article describes the German government's preparations in the field of cyber security, cooperation between German authorities, and preparations relating to personnel and reinforcements for the relevant institutions. The second part describes preparations at the security-military level and how Germany is adapting to the new challenges. The last part of the article examines the situation from an international angle and looks at how Germany sees its role as an international leader in the cyber field.

Keywords: Cybersecurity, Germany, strategy, government preparations, military preparations

Omree Wechsler is a researcher at the Yuval Ne'eman Workshop of Science, Technology, and Security and at the Blavatnik Interdisciplinary Center for Cyber Research, Tel Aviv University.

Cyber, Intelligence, and Security | Volume 2 | No. 1 | May 2018

Introduction

On February 23, 2011 Germany published its comprehensive cyber strategy. The document defines its perception of the cyber threat, determines guidelines for a cyber security strategy, and defines the goals and steps to implement them. The steps taken by Germany since the publication of this strategy in 2011 have focused on protecting critical infrastructures, increasing public awareness, making manufacturers responsible for supplying secured products, reinforcing IT security among government agencies, setting up the National Center for Cyber Defense (Cyber Abwehrzentrum – Cyber A-Z), establishing the National Council for Cyber Security, improving the efficiency of fighting crime in cyberspace, and positioning Germany as key actor in the efforts to provide cybersecurity in Europe and around the world.

In November 2016, the German cabinet approved a new strategy document on the subject of cybersecurity, which was published by the Ministry of the Interior. The new strategy is broader than its 2011 predecessor, with details about four main areas in which Germany must take action: safe and independent use of the digital environment; cooperation between the German state and the economic sector in the cyber field; building an effective cybersecurity architecture in the public sector; making Germany a central actor in the European and global cyber policies.

Perceiving the Threat

While the German strategic document of 2011 presented the cyber threat in fairly general terms and described the complexity of cyberattacks, in contrast, the 2016 document indicates the growing importance of Germany in the cyber field vis-à-vis the rise in the number of cyberattacks and their complexity. The 2016 strategic document deals, inter alia, with the social, economic, political, and personal damage caused by cyberattacks and describes them as a threat to stability, public order, and democracy. It also defines targets where the results of an attack would be particularly damaging, both publicly and privately. They include attacks on critical infrastructures, especially the energy sector and the power grid; attacks on banking infrastructures and financial institutions, and manipulations of the stock exchange; manipulation of autonomous systems, and of data traffic used by IT systems, such as in the field of health; and dissemination of false information, misleading reports, and fake news to manipulate public opinion and thus threaten free society and democracy.

The German Ministry of Interior, which as mentioned was responsible for drawing up the strategy, identified various types of cyberattacks and their motives: The motive for committing cyberattacks is broad and could be ideological or criminal. Attackers may be terror organizations, organized criminal gangs, military units, or intelligence services of other nation states. The varied background of the attackers and their level of professionalism render it very difficult to detect, monitor, and analyze attacks. The authors of the document warn against political or military conflicts that could be accompanied by hostilities in cyberspace. Such conflicts could escalate into a full-fledged cyber war, or even into cyberattacks just below the level of an armed conflict.

The overall picture suggests that an array of threats is composed of many players with different capabilities and motives. Therefore, the document's authors conclude that the classic means of protection for existing IT systems are not enough. They assume that the number of cyberattacks will increase, their complexity will grow, and the main targets of cyberattacks will be German society, economy, and industry, as well as German democracy.

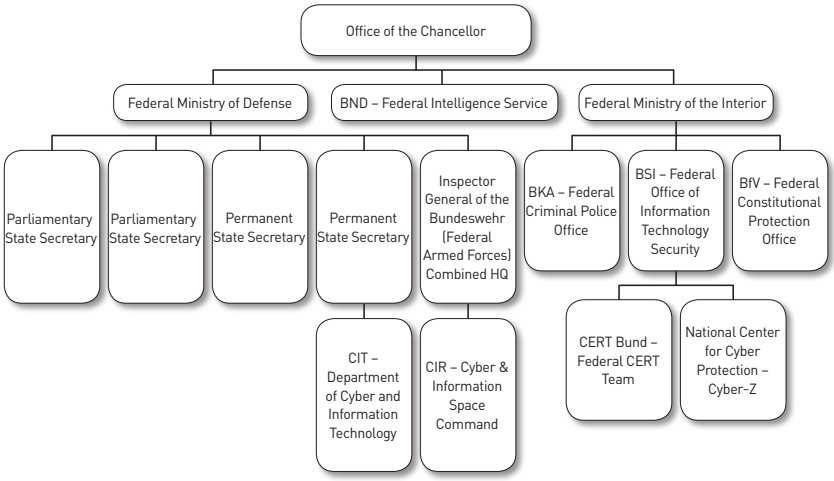

Diagram 1: Security and Cyber Entities in Germany

Government Preparations

Government entities responsible for the field of cyber in Germany are the Federal Office of Information Technology Security (BSI); the Federal Office for Protection of the Constitution, which acts as the internal security agency

(BfV); the Federal Intelligence Service (BND); the Federal Criminal Police Office (BKA); the Ministry of Defense (BMVg); the Ministry of the Interior (BMI); and the Federal Office of Civil Protection and Disaster Assistance (BBK), which corresponds to the Home Front Command in Israel.

The Office of Information Technology Security

The Office of Information Technology Security or the BSI (Bundesamt für Sicherheit in der Informationstechnik) is a federal office under the authority of the Ministry of the Interior, which also functions as a national cyber security authority. The BSI was set up in 1991, with the aim of providing IT services to government entities, IT system manufacturers and suppliers, and users. Today the BSI is responsible for protecting Germany's information technology and for implementing its national IT security policy. It is also responsible for a range of activities, such as early warning, prevention and incident response, issuing warnings on malware and vulnerabilities in products, establishing training channels, and raising awareness among government entities and the public. The office is also responsible for the information exchange between government ministries, institutions, and organizations in the private sector; formulating security standards for operators of critical infrastructures and products; and qualification and training processes for organizations and products.[1]

The BSI is responsible for other entities engaged in handling cyber threats, such as the National Center for Cyber Defense (Cyber A-Z), the Federal CERT Team (CERT-Bund), and the Civilian CERT (Bürger-CERT). The latter is responsible for increasing awareness of cyber threats among the public and small businesses.[2]

Strengthening the National Center for Cyber Defense

The National Center for Cyber Defense or the Cyber A-Z (Cyber Abwehrzentrum) is a federal institution designed to protect against electronic attacks on Germany's IT infrastructures and its economic sector. The center

1 Melissa Hathaway, Chris Demchak, Jason Kerben, Jennifer McArdle, and Francesca Spidalieri, "Germany: Cyber Readiness at a Glance," *Potomac Institute for Policy Studies* (October 2016), pp. 5–7; http://www.potomacinstitute.org/images/CRI/CRI_Germany_Profile_PIPS.pdf; "Cyber-Sicherheitsstrategie für Deutschland 2016," Bundesministerium des Innern, 2016, p. 17.

2 Hathaway et al., "Germany: Cyber Readiness at a Glance," pp. 5–7.

was set up following a cabinet resolution in February 2011 and began operating in Bonn in June that year, under the BSI.[3] The main tasks of the Cyber A-Z are to prevent cyberattacks and provide information and early warning of such attacks. The center shares information about profiles and identities of the people behind cyberattacks, and about the weaknesses of IT products.

The Cyber A-Z is not an independent entity but rather is the outcome of a number of cooperation agreements between German authorities engaged in cyber protection. Therefore, the separation between the jurisdiction and responsibility of the various authorities, particularly between the police and the intelligence services, is maintained while cooperating in the center's framework.

The 2016 strategy document recommends that Cyber A-Z should be further developed as a coordination center, and in the future be given the independent ability to analyze and prepare updates that will accurately describe real-time situations. It also recommends that the National Center for Cyber Defense should function as a center for shared training and exercises for how to cope with cyberattacks.[4]

Strengthening the analysis and response capabilities of government ministries

Germany is investing in the establishment of Mobile Incident Response Teams (MIRT), which are subordinate to the BSI. The purpose of these teams is to analyze the situation during an attack and help local teams to handle the incident and its consequences. The mobile teams provide assistance, by request, to constitutional bodies, federal authorities, and operators of critical infrastructures and important installations. The purpose of the assistance is mainly to mitigate incidents and threats, enable recovery, and to return to normal activity.[5] The MIRTs are supposed to receive assistance from special units of the Federal Criminal Police Office (BKA) and the Federal Office for Protection of the Constitution.

Other teams are supposed to be set up under the BKA. These teams, called Quick Reaction Forces, will form a legal unit whose role will be to

3 The authorities that play a central role in operating the Cyber A-Z: the BfV, the BSI, and the BBK. Other authorities that cooperate and are involved with the center's activity are the BKA, the BND, the federal police, and the army (the Bundeswehr).

4 "Cyber-Sicherheitsstrategie für Deutschland 2016," p. 28

5 Ibid, p. 29.

provide a fast response to cyberattacks through close coordination with the various state prosecutors in Germany or with the Federal Attorney's Office. The teams should accelerate processes of enforcement and arraignment, working with the German enforcement authorities.

The BfV has also set up Mobile Cyber Teams, consisting of IT experts and intelligence experts with experience of analyzing cyberattacks. These teams include people who are fluent in foreign languages and who deal with cyberattacks by foreign intelligence services and terror organizations.[6]

Strengthening existing CERT teams and setting up additional emergency response teams

As stated, the Federal CERT Team is a branch of the BSI with the responsibility of assisting the authorities, operators of critical infrastructures, businesses, organizations in the private sector, local authorities, and research institutions. In addition, the Federal CERT is responsible for maintaining contact and coordinating with foreign and international CERT teams.[7] The German government intends to invest additional resources to enlarge the Federal CERT Team and broaden the knowledge and expertise of its members, as well as setting up new CERT teams.

Strengthening the early warning capabilities of the German Federal Intelligence Service

The Federal Intelligence Service (BND) is responsible, inter alia, for monitoring and recording attempts by external elements—states, terror or criminal organizations—to carry out cyberattacks on Germany's infrastructures, as well as on its economic and civilian sectors. Monitoring and documenting attempted attacks should enable the BND to construct a model of how the attackers behave and thus provide early warning whenever suspicious activity on their part is detected.

The BND works with IT experts and analysts in order to build an early warning system for cyberattacks. The system is intended to identify potential attacks, analyze them, and build a map of threats. Early detection efforts are based on SIGINT, intelligence that is gathered by means of initiated internet scans as part of a policy dubbed "Signals Intelligence Support to Cyber

6 Ibid.

7 Ibid, p. 34.

Defense."[8] Development of the early detection system began in 2014, and by 2020 about 300 million euros will have been invested in this project. It is being executed in collaboration with the intelligence agencies of Germany's allies and is expected to provide a response to attempts at network espionage.[9]

The BND uses sensors installed on optical fibers all over the world. They give the German intelligence service the ability to track data traffic in other countries and to monitor cyberattacks in advance. This method also enables the German intelligence service to gather information about malware and to maintain a database of attack tools.[10]

Strengthening legal and constitutional frameworks in cyberspace

The German government is working to strengthen enforcement and judicial authorities in order to fight cybercrime. First, the government will be responsible for allocating resources to the relevant authorities and for the additional skilled manpower required in the fields of detection, criminology in cyberspace, and criminal identification in digital space. Secondly, the government will assist the security and enforcement authorities to develop and build analysis and assessment systems. Thirdly, special emphasis will be placed on matching the technology with the powers and means available by law to enforcement and juridical entities. The development of both aspects side by side is intended to avoid gaps between the law and the technology. Fourthly, the government will stress cooperation between German authorities and other countries, emphasizing exchange of information, professional knowledge, and experience between the German authorities and their counterparts in other countries and between those at federal and local level within Germany.[11] An example of the type of cooperation that Germany wishes to reinforce is the existing cooperation with the European Union in

8 Ibid, p. 32.

9 "300 Millionen für Frühwarnsystem gegen Cyberattacken," *Spiegel Online*, May 16, 2014, http://www.spiegel.de/netzwelt/netzpolitik/bnd-arbeitet-an-fruehwarnsystem-gegen-cyberattacken-a-969899.html.

10 Frederik Obenmaier and John Goetz, "Geheimdienst verstärkt Kampf gegen Cyber-Angriffe," *Süddeutsche Zeitung*, May 9, 2014, http://www.sueddeutsche.de/politik/abwehr-von-schadsoftware-geheimdienst-plant-fruehwarnsystem-fuer-cyber-angriffe-1.1956067#redirectedFromLandingpage.

11 "Cyber-Sicherheitsstrategie für Deutschland 2016," p. 30.

general and with specific EU entities, such as the EU Agency for Network and Information Security (ENISA) and the Europol Center for Cyber Crime.

Strengthening the powers of German entities that deal with cyber threats finds expression, inter alia, in enhancing the powers of the Federal Criminal Police Office and the Federal Police in the fields of cybercrime, cyber espionage, and so on. In addition, the German government has undertaken to reinforce and extend the Center for Cyber Crime operating within the framework of the Federal Criminal Police Office. The aim is to strengthen the center's abilities to investigate and assess situations and also to update the criminal law with more severe penalties for cybercrimes.

In order to deal with spying in cyberspace, the authority of the Federal Office for Protection of the Constitution will be enhanced, including improving its abilities to maintain more effective tracking and analysis of changing patterns of behavior shown by terrorists and extremist elements on the internet.[12]

Military Preparation

Two important organizational steps have been taken in the field of military security in order to improve Germany's preparations for dealing with the cyber threat: the establishment of the Cyber and Information Technology Department (CIT) of the Ministry of Defense and the establishment of an independent Cyber and Information Space Inspectorate (CIR), alongside branches of the military. These steps are intended to provide protection for military IT systems and to formulate military strategies that will render the security forces relevant in the digital age, by providing defensive and offensive cyber capabilities.

Cyber and IT Department

In September 2016, the Minister of Defense Ursula von der Leyen announced the establishment of a new department, Cyber und Informationstechnik (CIT). Klaus Hardy Muehleck was appointed head of the new department, with a staff of about 130.[13] The CIT will build a military cyber security layout

12 "Digitale-Agenda: Mehr Sicherheit im Cyberraum," *Bundesregierung*, 2014, https://www.digitale-agenda.de/Webs/DA/DE/Handlungsfelder/6_Sicherheit/6-5_Cyberraum/cyberraum_node.html.

13 Before his current appointment, Muehleck was chief information officer at Thyssenkrupp, chief information officer at Volkswagen (2004–2011) and responsible for information technologies at Audi (2001–2004).

based on the national cyber security strategy. It will also lead processes of professionalizing the German army in the field of data security and will be responsible for cyber and IT in the military field.

The CIT Department has two sub-departments: one in Berlin, which will handle cyber and IT governance, planning, and strategy in the field of information technology. Its tasks will include digital policy and managing IT initiatives. This department will also be responsible for building the IT system of the Ministry of Defense and the German army. The second sub-department will be set up in Bonn, and its purpose is to provide IT services and handle the implementation and routine operation of military IT systems. Other areas of responsibility will include protection of IT systems, passive cyber protection, and encryption security.[14]

Cyber and Information Space Command (CIR)

The Cyber and Information Space Command (Cyber und Informationsraum) was set up as part of the German army in November 2015. Its task was to examine organizational aspects, areas of responsibility, and tasks facing the German army (the Bundeswehr) in the fields of cyber and information. In October 2016, General Maier Ludwig Leinhos, a three-star general, was appointed to head the new command, and in April 2017, the CIR began to function as a military command headquarters in every way. It is expected to become fully operational by the start of 2021. The CIR began its activity with an initial staff of about 260 people, which by July 2017 had grown to about 13,500 people. This is expected to increase to about 14,500 in 2021. 1,500 of the posts are reserved for civilians.[15]

The tasks of the CIR are defined as passive and active defense in cyber and information space. The German army is a sensitive target for hundreds of daily cyberattacks, first and foremost aimed at stealing information and data and to interfere with IT-supported weapons systems. The Bundeswehr's central importance to the NATO alliance also makes it a target for hackers. Because of this sensitivity, the primary aim of the CIR is to protect the Bundeswehr's networks and IT systems. Passive defense involves monitoring,

14 "Verteidigungsministerin stellt neue Cyber-Abteilung auf," *Bundesministerium der Verteidigung,* October 5, 2016.

15 "German Military to Unveil New Cyber Command as Threats Grow," *Reuters*, March 30, 2017, http://www.reuters.com/article/us-germany-military-cyber/german-military-to-unveil-new-cyber-command-as-threats-grow-idUSKBN1712MW.

early detection, analysis, and assessment of damage, plus the ability to neutralize the threat and assist in the return to normal function. The CIR's other tasks are to protect government institutions, public entities, and critical infrastructures against cyberattacks from foreign elements, such as nation states and terror organizations, as well as the struggle against propaganda, disinformation, and fake news.

In addition to passive defense, the Bundeswehr is developing offensive capabilities that it defines as "active defense." These are expressed in the ability to collect intelligence about foreign networks and systems and to interfere with their operation. These offensive capabilities are still being developed and are under the responsibility of the CNO (Computer Network Operations) team, composed of about eighty experts, graduates of the computer science departments in the Munich Military Academy, who specialize in hacking into networks and servers, carrying out manipulations and causing damage.[16] Although the CNO team has existed since 2009, under the Cyber and Information Space Command, it has been extended and transferred from the Operations Department of the Bundeswehr Strategic Command to a new cyber operations center and its capabilities in the field of scanning networks, collecting intelligence, and enemy simulation are expected to grow.

These capabilities of the German army have aroused a lively debate among legislators in Germany and drawn criticism from the public, which is mostly against the use of force and fearful of entering a "cyber war" or cyber arms race and is therefore suspicious of the idea of providing additional powers and capabilities to the security forces. Indeed, the offensive capabilities represent a fundamental change in the German security concept, making it more pro-active than previously.[17]

Recruitment system for the Cyber and Information Space Command

The Bundeswehr works with the Ministry of Welfare and Development in the field of recruiting new personnel for the CIR. The intention is to create a mechanism for recruitment and employment that will include career development tracks for the recruits and operate with the dynamism and

16 Christian Kahl, "Vom Kampf in der fünften Dimension," *Bundeswehr Journal*, May 3, 2013, http://www.bundeswehr-journal.de/2013/vom-kampf-in-der-funften-dimension.

17 Isabel Skierka, "Bundeswehr: Cyber Security, the German Way," *Digital Frontiers* (blog), *Observer Research Foundation*, October 20, 2016, http://www.orfonline.org/expert-speaks/bundeswehr-cyber-security-the-german-way/.

flexibility that characterize the IT market. The aim is to achieve the target number of recruits and train personnel who can use their initiative and think flexibly. The idea of addressing target groups that until recently were not candidates for recruitment—including people who were found unsuitable for a military framework, people from immigrant families, holders of dual citizenship, dropouts from formal education, and candidates in other professional fields—is also being considered. Recruitment devices to find suitable candidates include competitions and tournaments to discover IT talents, start-up competitions, recruitment of candidates from the field of gaming, and the provision of scholarships for relevant studies.[18] The Bundeswehr has also set up a research department, the Cyber Cluster, at the Munich Military Academy, and launched a program of studies for a degree in cyber security, which is expected to produce about seventy graduates each year.[19]

The International Arena

Germany sees the international arena not only as an opportunity to strengthen its cyber security through partnerships and joint initiatives but also as a platform for strengthening its economy and industry, which is largely based on exports. Germany's positioning at the center of the international arena in the field of cyber and IT reinforces its reputation and political status all over the world. In the strategy document of 2016, the German government seeks to position itself at the forefront of the regional-European and international efforts to build resilience, handle cyber threats, and define standards for cyber security.

There are four main areas in which Germany intends to promote its cyber security policy: Europe and the European Union; NATO; the international arena; and bilateral co-operations.

Europe: The security of the European market and the regular continuity of trade on the continent are the greatest interests of the German government. With the growth of digital trade, the question of cyber security for the European single market is also gaining importance. An overlap exists between the German interest in securing the online economy, the networks and information systems that are being used, and the interest of the European

18 "Abschlussbericht Aufbaustab Cyber- und Informationsraum," *Bundesministerium der Verteidigung*, April 2016, pp. 31–33.

19 Ibid., pp. 35–36.

Commission, whose purpose is to create trust and security in the projects of the European Union, including the digital single market.

Another of Germany's interests is to preserve human rights and privacy when using the internet. Against this background, the German government announced its support for European Commission regulations to regulate the transfer of data and information within Europe and to protect privacy and commerce.[20]

The government is also working to strengthen Germany's status in the framework of European cyber policy, through its growing involvement in the EU foreign and defense policy. The German government supports the promotion of research by German academics in the field of IT security and works to connect them with their counterparts all over Europe, as well as promoting the local IT industry. A large part of promoting the German industry and increasing Germany's involvement in shaping the EU cyber security policy finds expression in support of EU projects dealing with legal and technical issues relating to cyberspace, such as the use of electronic identification and signatures by businesses and authorities. This makes it possible to identify users and provides full cooperation with the European Union Agency for Network and Information Security (ENISA).[21]

NATO: Germany's foreign and defense policy considers NATO as the backbone upon which the Euro-Atlantic alliance rests. Germany's membership ensures both its security and that of Europe. According to the German strategy, the collective security concept of NATO also applies in cyberspace, and therefore NATO must also become capable in cyberspace, alongside the spheres of sea, air, and land. Germany is a leading partner in the processes of building NATO's cyber security formation and of an effective deterrence policy in cyberspace in the face of threats of "hybrid" warfare; that is, the combination of kinetic and cyber warfare.[22]

The international arena: Germany has positioned itself as a leader of discussions in international organizations, headed by the Organization of Security and Cooperation in Europe (OSCE) and the United Nations (UN) on matters affecting compliance with international law in cyberspace; closing cyber loopholes in international law; developing norms, regulations, and

20 "Cyber-Sicherheitsstrategie für Deutschland 2016," p. 40

21 Ibid.

22 Ibid.

principles concerning responsible conduct by states in this field; and also reinforcing the capabilities and authority of the UN in cyberspace.

Other areas where Germany plays a part is in raising awareness of the risks in cyberspace; expanding frameworks for sharing information on cyberattacks and incidents; reinforcing the international response; increasing the severity of penalties for economic espionage and cyberattacks; and actively supporting stronger supervision of the export of technologies that can be exploited for offensive behavior in cyberspace.[23]

Bilateral contacts: Germany works to support its partners and help them to build capabilities for detecting, preventing, and responding to cyber incidents, and strengthen their digital infrastructures. As part of Germany's efforts to be perceived as a reliable player in the international arena, it encourages other players to introduce legislative reforms on cyber matters, sign treaties and take confidence building measures to strengthen cyber security.[24]

The Challenges and Potential Consequences of Germany's Preparations

Notwithstanding the various preparations, the increased manpower and the widening of powers for various authorities and other entities, the German government still faces a number of challenges in cyberspace. Some of these are legal constraints affecting the use of offensive cyber capabilities and cooperation between the army and intelligence and espionage units, while others are the gaps in the realm of employing a professional workforce. Germany's preparations in cyberspace also have several potential consequences for its ambitious foreign and defense policy in the international arena.

Constitutional gaps regarding the use of force

As part of the military restraint that has characterized Germany since the end of World War II, the German constitution states that any use of military force for purposes that are not purely defensive requires a parliamentary mandate. A report from the German Ministry of Defense states that the need for the parliamentary mandate is also valid for operations in cyberspace.[25] Due to the complexity of this space, where it is not always possible to distinguish

23 Ibid, p. 41.

24 Ibid, p. 42.

25 "Abschlussbericht Aufbaustab Cyber- und Informationsraum," p. 5.

between defensive and offensive moves, questions arise as to how and in which cases the army must turn to parliament for its approval. It appears that the section in the constitution requiring parliamentary approval for active defense operations or a preemptive strike could pose a challenge to cyber operations, particularly in the case where rapid, covert responses are needed. A means of bridging these gaps has not yet been found.

Cyberattacks require accurate intelligence about target networks and systems and about weaknesses that can be exploited. Such intelligence as well as spying and other actions required to prepare for a cyberattack is the province of the intelligence services. Therefore, the German army will have to cooperate and share information with the German espionage and intelligence services. In the United States, such cooperation is seen as obvious, particularly since the US Cyber Command shares the same leadership with the National Security Agency (NSA) and uses its assets and the intelligence it provides; such cooperation in Germany, however, faces severe constitutional constraints. Although the legal dimension of cooperation between intelligence units and the army and enforcement agencies in Germany is beyond the framework of this paper, it should be noted that there is a legal debate over the types of information that espionage entities, particularly the BND, are permitted to share with other German authorities.[26] Moreover, the BND is subordinate to the Office of the Chancellor, while the army is subordinate to the Ministry of Defense, and the Federal Office for Protection of the Constitution is subordinate to the Ministry of the Interior. Therefore, it is not clear how they will be able to maintain cooperation. Furthermore, there is still no definition of the division of powers between these three entities regarding the collection of data relating to cyber operations.

Challenges of recruiting skilled personnel

Another problem that is not unique to Germany is recruiting and training personnel to fill the new jobs in the CERT teams, and particularly in the Cyber and Information Space Command of the Bundeswehr. In spite of the announcement by the German army that the Cyber Command has already been staffed by soldiers selected from other branches of the military, the

26 Kai Biermann, "BND-Überwachung: Warum schickt der BND der Bundeswehr abgehörte Daten?" *Zeit Online,* March 18, 2015, http://www.zeit.de/politik/deutschland/2015-03/bnd-bundeswehr-daten-ueberwachung/komplettansicht.

Bundeswehr still faces the challenge of setting up a reserve pool for the new command. In a letter from the federal office responsible for military armaments and equipment to reserve soldiers in the field of IT, they were asked to give names of civilian colleagues in the field.[27] The letter also stated that the army needed hackers, IT developers, IT security experts, penetration testers, and more.[28]

Apart from the difficulty of recruiting talented and experienced IT people, the Bundeswehr suffers from low recruitment rates and has an image of being an unattractive employer. There has also been criticism of the army's ambitious plans, with claims that it is insufficiently flexible and that its pace of training, procurement, and equipping itself does not match the pace of initiative and innovation in hardware and software markets, nor the rapid pace of change in cyberspace.[29]

The academic curriculum launched by the Bundeswehr to train IT people is a positive step in the right direction, but given the expectation of about seventy graduates from the program each year, it appears that it will take a long time before the army's needs are met. In this situation, there is a fear that the Bundeswehr will have to turn to private contractors to perform some of the jobs. This option raises worries about maintaining national security, given the many examples of leaks and national security breaches through contracted staff working for the NSA in the United States.

Opportunities in the international arena

Germany's ambitions and its wish to leverage its international status as well as its economy and industry are not new. In recent years, Germany has actively and consistently participated in international forums dealing with cyber security, information and communications technologies, such as the UN, the European Union, NATO, the G7 summit, the European Organization

27 The Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support.

28 Matthias Monroy, "Herausforderungen im Cyber- und Informationsraum: Bundeswehr sucht Tips für Aufbau einer Cyber-Reserve," *Netzpolitik,* April 26, 2016, https://netzpolitik.org/2016/herausforderungen-im-cyber-und-informationsraum-bundeswehr-sucht-tips-fuer-aufbau-einer-cyber-reserve/.

29 Nina Werkhäuser, "German Army Launches New Cyber Command," *Deutsche Welle*, April 1, 2016, http://www.dw.com/en/german-army-launches-new-cyber-command/a-38246517.

for Security and Cooperation, and others. Germany has also taken part in dialogues concerning the development of cyber capabilities and has actively participated in the discussions of the UN Group of Governmental Experts (GGE) to define norms of conduct in cyberspace.

Germany's bilateral activity has been and is still characterized by providing aid on cyber matters to developing countries and by cooperating on these matters with developed countries.[30] Examples can be found in the talks held in Berlin with delegations from India;[31] in the signing of a cooperation agreement with the Estonian Defense Industry Association;[32] and in the cooperation agreement with Singapore on cybersecurity.[33]

In addition to these trends, which are expected to continue, Germany has found new opportunities in the international arena: President Trump's "America First" policy and the ongoing lack of clarity regarding the United States and its relative distance from the European Union and NATO, at least in comparison to the Obama administration, could give Germany the opportunity to play a more central role in the leadership of the western countries. Specifically, the closure of the Office of the Cyber Security Coordinator in the US State Department in 2017, which could be seen as damaging the diplomatic capabilities of the United States in the field of cybersecurity, could be an opportunity for Germany's ambitious foreign policy.[34]

The possible exit of Britain from the European Union will apparently lead to gaps in the EU security and intelligence gathering. This is also true for cybersecurity. The vacuum left by the departure of Britain—considered

30 Hathaway et al., "Germany: Cyber Readiness at a Glance," p. 13.

31 "Indo-German Intergovernmental Consultations in Berlin—Strengthening Cyber Cooperation," *German Missions in India*, May 31, 2017, http://www.india.diplo.de/Vertretung/indien/en/__pr/Politics__News/Merkel__Modi__2017__update2.html.

32 "Cyber-Security Council Germany and Estonian Defence Industry Association sign cooperation agreement, agreeing upon fostering transnational cooperation in the area of cyber security together," *Cyber-Security Council Germany*, September 14, 2017, http://www.cybersicherheitsrat.de/data/PRESS-RELEASE-Cyber-Security-Council-Germany-and-Estonian-Defence-Industry-Association-sign-cooperation-agreement.pdf.

33 Prashanth Parameswaran, "What's in the New Singapore-Germany Cyber Pact?" *The Diplomat*, July 11, 2017, https://thediplomat.com/2017/07/whats-in-the-new-singapore-germany-cyber-pact/.

34 Morgan Chalfant, "Tillerson Moves to Close State Cyber Office," *The Hill*, August 29, 2017, http://thehill.com/policy/cybersecurity/348438-tillerson-moves-to-close-state-cyber-office.

a central player in this field—could encourage Germany to step in with its capabilities. The British exit could harm not only cybersecurity but also the whole range of information sharing between EU countries, including Germany.

Conclusion

Germany sees the cyber threat as paramount and is therefore preparing to protect its economy, industry, security forces, and critical infrastructures. It is doing so through a range of actions on various fronts: legal, constitutional, military, federal, and local. Germany's comprehensive strategy published in 2016 specifies the main steps intended to provide a response to the cyber threats it faces. This strategy supports strengthening and expanding entities and units for cyber protection and renewed military preparation, including setting up specialist entities for cyber defense.

In the area of government preparations, Germany emphasizes expanding existing bodies and reinforcing their capabilities. A striking example is the expansion of the National Center for Cyber Defense (Cyber A-Z), which acts as the link between government ministries that are legally responsible for cyber activity, and also the granting of independent capabilities to this unit for the purpose of analyzing, assessing, and defining the situation as well as adding a platform for practicing and simulating emergencies. Other examples include the reinforcement of local response capabilities by means of federal aid.

In the military arena, Germany set up the Cyber and Information Technologies Department that operates under the Ministry of Defense. The department is responsible for strategic military cyber planning and for building the Bundeswehr cyber security layout. It also set up the Cyber and Information Space Command, which is responsible for protecting the army's networks and IT systems and is intended to be equipped with both defensive and offensive capabilities. Its potential offensive capabilities represent a significant change in German policy, which until now had avoided using force and building offensive capabilities as it could arouse public criticism.

In the international arena, Germany apparently sees international and bilateral cooperation not only as a strategic move to strengthen national cyber security but also as an opportunity to leverage and reinforce its economic and political status in Europe with its bilateral partners and international organizations by playing a major role in the joint effort to handle cyber

challenges. Positioning itself as a cyber power is Germany's attempt to strengthen its international, political, and diplomatic standing, as well as its industry and technology and export-based economy.

Germany joins a long line of European countries, including Britain and France, that are worried about espionage, data theft, instability, external influences on public opinions, and foreign intervention in their democratic processes and therefore are choosing to invest efforts and resources to mitigate these threats. However, there are constitutional challenges to Germany's strengthening in the field of military cyber, and particularly the use of offensive cyber weapons and the principles of active defense, which is part of the role of the new CIR. Other challenges in the areas of equipment and personnel are evident, but they are not unique to Germany. The partial measures taken to deal with these challenges are a step in the right direction but are not expected to provide a complete solution to the problem.

Germany is undergoing an interesting process, mainly due to its power and centrality to European and international politics and economy. It is possible that events with international influence, such as the Trump Administration's "America First" policy, will force Germany to increase its security expenditure, which includes cyber defense and cyber warfare. Other events, such as the British exit from the European Union, are expected to affect Germany's security in general and its cyber security in particular, since it is linked to the security of the entire European Union.

Another interesting process is the deep change in Germany's security concept, which in spite of constitutional challenges, is increasingly based on active defensive and offensive means. This is a tremendous change for a country that has avoided the use of force for the last seventy years. This change, however, is expected to encounter many opponents, both within the German public and legislature, making it harder to implement.

The Cybersphere Obligates and Facilitates a Revolution in Intelligence Affairs

David Siman-Tov and Noam Alon

History is replete with examples of world powers, countries, and militaries that failed to identify the revolutionary potential of a new technology and, as a result, lost their advantage and relevance. This article addresses the gap between the essential technological changes that the cybersphere has created and facilitates and the outmoded functioning of intelligence organizations, which have remained rooted in the approaches, architecture, and tenets of the intelligence cycle paradigm that emerged between the two world wars. This gap creates a need for a systemic and conceptual change, but the lack of an awareness of crisis and urgency within the intelligence community as well as in the public discourse has delayed any transformation, even though discussion about the gaps between the functioning of the intelligence agencies in the cyber age and their approaches, culture, and structure has been underway for more than a decade. The main reason for this lack of awareness of crisis and urgency is that the intelligence community continues to function and make achievements even in its current format, particularly in operative and tactical spheres.

This article is significant in that it provides a clear and methodical presentation of the gaps and tensions in the intelligence community due to its delay in adopting a new paradigm.

Keywords: Intelligence, cybersphere, revolution in intelligence affairs, intelligence community, paradigm, intelligence cycle

David Siman-Tov is a researcher at the Institute of National Security Studies. Noam Alon is an expert in the fields of strategy and intelligence.

Introduction

History is replete with examples of world powers, countries, and militaries that failed to identify the revolutionary potential of a new technology and, as a result, lost their advantage and relevance.[1] The history of business companies is awash with similar stories that also resulted in the collapse of mega corporations and the rise of other corporations in their stead.[2] This history proves that merely identifying and adopting new technologies is not enough, since conceptual, cultural, structural, and value-laden changes are needed to fully realize the technological potential and crystallize it into a revolution that creates a new paradigmatic operational space.

This article addresses the gap that developed between the material technological changes that the cybersphere—in its broadest sense—has facilitated, including new approaches to the production of information and knowledge, the interactions between intelligence organizations and the environment and their intelligence targets, and the modus operandi of the intelligence organizations. To a great extent, these organizations have remained rooted in their approaches, architecture, and tenets from the intelligence cycle paradigm that emerged between the two world wars.[3] This gap creates a need for a systemic and conceptual change, but the absence of awareness of crisis in the intelligence community as well as in the public discourse has delayed this transformation. This lack of an awareness of crisis is mainly due to the fact that the intelligence community continues to function and achieve results, particularly at the operative and tactical levels. Another reason for the absence of change in the existing paradigm is because the public and many decision makers perceive the intelligence community as a "black box," inhibiting any critical discourse that could motivate change from outside.

---

1 Max Boot, *War Made New: Weapons, Warriors and the Making of the Modern World*, (Tel Aviv: Maarachot Publishing, 2015) [In Hebrew].

2 Well known examples are the collapse of both Kodak and Blockbuster due to their failure to adapt to the digital age, and Blackberry's loss of its dominance because of its fixation on the structure of its digital device.

3 The concept of the "intelligence cycle" defined a number of basic stages that comprise the intelligence process: information collection, information processing (i.e., analysis), and distribution of the resulting intelligence to the various consumers. For more on this subject, see David Siman-Tov and Ofer G., "Intelligence 2.0 – New Approach to the Production of Intelligence," *Military and Strategic Affairs* 5, no. 3 (December 2013): 27–29.

The Current Intelligence Paradigm: "The Intelligence Cycle"

A paradigm is a world view that defines the conceptual perspective and the structure and logic of the basic functions of a system and its components. The conceptual perspective is based on the social and organizational consensus that determines the relations between the various parties and explains and interprets the environment in which the individual and the organization operate.[4] Paradigms are challenged and naturally change as disparities multiply between the customary interpretation and the phenomena that it is supposed to interpret; however, any such change also triggers a crisis, due to the difficulty in adopting new perspectives and discarding the old ones. As soon as a new paradigm is formulated, it presents a conceptual system of beliefs, values, and concepts, and these are reflected in structures, processes, ethics, and the boundaries of what is permitted and prohibited. Well known historic examples of changing paradigms are the shift from the belief in faith and myths to the need to prove things scientifically and the shift from the assumption that the earth is flat and at the center of the universe to the recognition of the centrality of the sun and that the earth is round.

In the military context, it is customary to mention the "Revolution in Military Affairs" (RMA) in the information age, which conceptually transformed the way militaries fight.[5] In the intelligence context, military leaders in the old world directly managed intelligence. This was Moses' role in the biblical spy affair as well as Napoleon's role. Within the scope of this paradigm, intelligence was based on relations of trust between the leader and the human spies that he operated. A new paradigm emerged during the industrial age, which produced, inter alia, the invention of the telegraph and walkie-talkies. This paradigm focused on the ability to collect and decode signals (a representative example of this is the Enigma Code, the key intelligence project during World War II).[6] The new paradigm required

4 Thomas S. Kuhn, *The Structure of Scientific Revolutions* (Chicago: University of Chicago Press, 1970), 2nd ed., pp. 52–76; Amir Levy and Uri Merry, *Organizational Transformation: Approaches, Strategies, Theories* (Greenwood Publishing Group, 1986), pp. 10–14.

5 Deborah G. Barger, *Toward A Revolution in Intelligence Affairs* (Santa Monica: RAND Corporation, 2005).

6 David Kahn, *Seizing the Enigma: The Race to Break the German U-Boats Codes* (New York: Houghton Mifflin Harcourt, 1991).

establishing a more professional intelligence organization that would be based solely on direct communications with the military leader. This is how the intelligence profession developed on the political level. The dramatic increase in the volume of signals and in electronic warfare necessitated the establishment of intelligence organizations that would engage not only in collecting and analyzing information but also in organizing, interpreting, and making information accessible to the decision makers. This is the paradigm that was employed when strategic intelligence organizations were established after World War II, with one of its key principles being the concept of the intelligence cycle as the logic that organizes the relations between the collection and research entities and between the intelligence organization and the leader.[7]

The intelligence cycle paradigm, which still prevails today to a great extent, differentiates between the various components of the intelligence system and defines the modes of communication between the various types of units within the intelligence organization, especially between the collection personnel and the researchers. Within the collection unit, it has created sub-divisions distinguished by the various modes of information collection: signals collection (SIGINT), open-source collection (OSINT), visual collection (VISINT), and human collection (HUMINT). The intelligence cycle paradigm also has determined the communication between the various units of the intelligence organization as well as with the decision-making echelon. These communications are characterized by questions and answers and by the strategic echelon's guidance and direction of the intelligence system (evaluating critical information).[8] It also sets clear boundaries between the object of the intelligence—another country or adversary that constitutes an object of intelligence activity—and the country where those intelligence

7 The main proponent of the concept of the intelligence cycle was Sherman Kent, who was the head of the CIA's Research and Analysis Branch and previously had developed his world view in academia. See Sherman Kent, *Strategic Intelligence for American World Policy* (New Jersey: Princeton University Press, 1949).

8 Ibid.

organizations operate.[9] The main role of intelligence is to provide factual answers and to expose secrets about the reality "on the other side" and mainly to provide warnings.[10]

Attempts to Contend with the Changing Reality

The dominance of the intelligence cycle paradigm presently is reflected in the organizational structure, the functional divisions, and the ethos and logic that govern the intelligence work. However, in recent years, the intelligence environment began functioning differently, which in many cases has been inconsistent with the principles of the intelligence cycle. Thus, a situation has emerged whereby, on the one hand, the intelligence components and the defined relations between themselves and with the external environment have remained as they were; yet, on the other hand, new and different components and patterns began to emerge that have challenged the existing paradigm. This is characteristic of the situation whereby the paradigmatic system is in an interim phase: it does not change the basic conceptual system that defines it; at the same time, however, it allows the "weeds" to grow but also attempts to contain them so that they do not challenge the mainstream.

In fact, calls for a "revolution in intelligence affairs" already were heard more than a decade ago. At the time, a main argument was that the intelligence organizations' major failures of the previous decades were the result of the changes in the strategic environment and in the nature of the challenges and threats.[11] Authors of a comprehensive research conducted by the RAND

9 For a first-hand description of the paradigm and its implementation in the Israeli case, see Yehoshofat Harkabi, *Intelligence as a Government Institution* (Tel Aviv: Maarachot Publishing, 2015) [in Hebrew]. Prior to the establishment of the State of Israel, and in the absence of defined borders, the intelligence service of the Yishuv used to frequently travel to the capitals of the Arab countries in order to seek answers to questions that troubled the leaders of the Yishuv. They also considered intelligence as "a bridge to peace." After the establishment of the state, this mission was replaced by the primary mission of developing knowledge about Israel's adversaries, the strategic environment, expressed mainly by providing warnings of war.

10 Joseph S. Ney, "Peering into the Future," *Foreign Affairs* 73, no. 4 (August 1994): 82–93.

11 David T. Moore, *Sense-making: A Structure for an Intelligence Revolution* (Washington, DC: National Defense Intelligence College, March 2011); Russell E. Travers, "Waking Up on another September 12th: Implications for Intelligence Reform," *Intelligence and National Security* 31, no. 5 (2016): 746–761.

Institute at the beginning of this century expressed concern that the actions of the US intelligence following its failure to prevent the terrorist attacks of September 2001 and its erroneous assessment of Iraq's nonconventional weapons were merely reforms of the old intelligence paradigm and were insufficient to bring about a real change in the functioning of the intelligence community.[12] The actions included establishing an umbrella organization tasked with determining the intelligence strategy and directing the intelligence community (the Directorate of National Intelligence [DNI]) and forming joint research entities. The DNI also began to encourage information sharing between the various intelligence organizations.[13]

The Israeli intelligence community also attempted to improve the intelligence functioning, inter alia, by using new systematic ideas, which included structural and functional changes. These included organizational restructuring processes implemented by the heads of the Military Intelligence Directorate led by Major-General Aharon Ze'evi-Farkash and by Major-General Aviv Kochavi.[14] The process that Major-General Ze'evi-Farkash conducted included the formation of joint intelligence forums, led by a

12 Barger, *Toward a Revolution in Intelligence Affairs*; Gregory F. Treverton and Peter A. Wilson, "True Intelligence Reform Is Cultural, Not Just Organizational Chart Shift," *RAND Blog*, January 13, 2005.

13 Gordon Nathaniel Lederman, "Restructuring the Intelligence Community," in *The Future of American Intelligence*, ed. Peter Berkowitz (Stanford: Hoover Press, 2005), pp. 65–102. In his article "Waking Up on Another September 12th: Implications for Intelligence Reform," Russell Travers seeks to expand this trend so that it will include the entire American intelligence community. According to his approach, three major courses of action need to be taken: subordinate all US intelligence agencies to a single intelligence director who is vested with full responsibility and authority; establish supra-organizational taskforces above the existing intelligence agencies, which will handle all of the national challenges; and enable a relatively free flow of information and knowledge between the different agencies and the supra-organizational task forces.

14 Aviv Kochavi and Eran Ortal, "*Ma'asei Aman*" – Permanent Change in a Changing Reality," *Bein Haktavim* (Dado Center), no. 2 (July 2014) [in Hebrew]; Aharon Ze'evi Farkash and Dov Tamari, *And How Will We Know* (Tel Aviv: Yedioth Ahronoth Publishing, 2011) [in Hebrew]; Naomi Fassa Yosef and Sarit Shapira, "Bridge over Troubled Water: The Aman Endeavor in the World of Complexity," *Intelligence in Theory and Practice* (Israeli Intelligence Community Commemoration and Heritage Center), no. 2 (2017); Hagai Huberman, "The Director of the Israel Security Agency: To Adapt Our Assessments to the Changing Reality," *Arutz 7*, May 15, 2011, https://www.inn.co.il/News/News.aspx/219724.

head of the research division, for the purpose of designing an intelligence campaign. This process expired after a few years. Among the changes directed by Major-General Kochavi was the establishment of a social network for intelligence purposes (nicknamed "Tracebook," with Facebook being its source of inspiration); however, personnel in the intelligence system today claim that the network's potential is only being partially realized and that the intelligence discourse on the network is limited. The director of the Military Intelligence Directorate, Major-General Amos Yadlin, established the Operations Division for the purpose of improving the ability of the Intelligence Division to engage in operative issues and improve the joint functioning of its collection and research personnel.[15] On the other hand, the attempts to form joint task forces in the Military Intelligence Directorate encountered difficulties and constant tension vis-à-vis the collection units. The intelligence discourse in Israel raised the idea of creating shared spaces for the production of intelligence knowledge, as well as the need to break the intelligence cycle by exploiting new technological capabilities to improve the intelligence functioning and enable it to more easily contend with the environment's new challenges. These ideas have not yet come to fruition, and as a result, most of the intelligence knowledge continues to be developed in each separate research organization.[16]

In recent years, additional complaints have been raised about the functioning of the intelligence community, emphasizing the need for a systemic change. For example, some point out that the information and big data age requires intelligence organizations to make systematic adjustments that are not always compatible with their current structure and functioning.[17] Others call for a change in the intelligence collection field, inter alia, by giving expression to the idea of all-source intelligence.[18] Furthermore, there has been growing recognition of the importance of open-source intelligence and the need to

15 Amir Rappaport, "Upheaval in Intelligence," *Israel Defense*, March 2014 [in Hebrew].

16 Siman-Tov and Ofer G., "Intelligence 2.0 – New Approach to the Production of Intelligence," pp. 27–42.

17 Kevjn Lim, "Big Data and Strategic Intelligence," *Intelligence and National Security* 31, no. 4 (2016): 619–635.

18 Roberto Mugavero, "Challenges of Multi-Source Data and Information New Era," *Journal of Information Privacy and Security* 11, no. 4 (2015): 230–242.

establish new intelligence centers that will specialize in this field.[19] Calls for the establishment of intelligence centers that will synthesize intelligence from multiple sources have also increased.[20]

Intelligence researcher William Lahneman called for a paradigmatic change in the American intelligence community, due to the changing access to information as well as the nature of the threats (the emergence of supra-state and sub-state threats). According to his approach, organizational, conceptual, and process changes that reflect a more decentralized and less compartmentalized approach are necessary, and, by doing so, they will help develop agility in the face of the changing reality.[21] In a comprehensive research study, Lahneman enumerated the reasons why the reforms instituted by the American intelligence community after the 9/11 terrorist attacks were inadequate, arguing that they were merely evolutionary changes and that subsequently, the US intelligence agencies continued operating according to the traditional Cold War era paradigm. According to Lahneman, a systemic transformation is needed, given the changing nature of the threats and the opportunities as a result of integrating forces and knowledge sharing with the civilian environment. Lahneman proposed that two paradigms be maintained concurrently: the traditional paradigm, which would focus on solving puzzles through covert and classified sources, and a new paradigm that would contend with global trends and new threats challenging both the intelligence community and state and global civilian organizations and would also enable cooperation with private business entities by employing a new

19 Hamilton Bean, *No More Secrets: Open Source Information and the Reshaping of U.S. Intelligence* (Santa Barbara: Praeger, 2011); Michael Glassman and Min Ju Kang, "Intelligence in the Internet Age: The Emergence and Evolution of Open Source Intelligence (OSINT)," *Computers in Human Behavior* 28, no. 2 (March 2012): 673–682; Hamilton Bean, "The DNI's Open Source Center: An Organizational Communication Perspective," *International Journal of Intelligence and Counterintelligence* 20, no. 2 (2007): 240–257.

20 Christopher G. Pernin, Louis R. Moore, and Katherine Comanor, *The Knowledge Matrix Approach to Intelligence Fusion* (Santa Monica: RAND Corporation, 2007).

21 William J. Lahneman, *Keeping U.S. Intelligence Effective: The Need for a Revolution in Intelligence Affairs* (Lanham, PA: The Scarecrow Press, 2011); William J. Lahneman, "The Need for a New Intelligence Paradigm," *International Journal of Intelligence and Counter Intelligence* 23, no. 2 (2010): 201–225.

concept of the flow of information. Robert Steele also addressed the need for sharing intelligence information with global civilian entities.[22]

The Cybersphere Penetrates the Paradigm's Boundaries

Despite the partial success of the attempts described above, after more than a decade, the conditions are now ripe for revolutionizing the way in which the intelligence communities are built and operate around the world as well as the relations between them and the external environment. What facilitates such a transformation and actually obligates it is the cybersphere, which, in the broad sense of the word, is "the missing piece" in the ideas that had been proposed in the past.[23]

The cybersphere includes the physical and non-physical space created by the following sources: computers, mechanized systems and networks, software, computerized information, content, and the users themselves.[24] At issue is a human, technological, and cultural phenomenon that emerged more in the last decade. The cybersphere is an artificial space (as opposed to sea, air, and land) and the communication between its components is carried out through bytes. This facilitates the creation of links and shared spaces between different intelligence disciplines, which in the past were compartmentalized and were only connected through people's minds.

Cybersphere, as a new intelligence environment, is changing the basic assumptions about information and knowledge. The volume of information that is available to intelligence agents—whether working in a research unit or in a collection unit—makes it impossible to know how much information exists on a particular subject, how much of the information they possess, and

22 Robert Steele, "Foreign Liaison and Intelligence Reforms: Still in Denial," *International Journal of Intelligence and Counterintelligence* 20, no. 1 (2007): 167.

23 "Information warfare is more than just information-enabled warfare, which albeit represents an important aspect of information or cyber warfare, but not in totality. Cyber warfare [should be perceived] as strategic warfare which can be used as a principle means to achieve strategic ends and as required by Luttwak's criterion for strategic warfare, the framework for the strategic cyber warfare is to be defined across all spectrum of affairs right from the grand strategy to the tactical level." The quote is taken from Amit Sharma, "Cyber Wars: A Paradigm Shift from Means to Ends," *Strategic Analysis* 34, no. 1 (February 2010): 62–73.

24 The definition is taken from an *ITU Cybersecurity Gateway* document.

whether they have all the relevant information.[25] Moreover, the intelligence organizations are incapable of fully utilizing most of the information in their possession, whether due to the deluge of information and knowledge from sensors or to the difficulty of contending with classified and non-classified databases. This state of affairs casts a dark shadow over the capacity to sustain the basic idea underpinning the architecture and functioning of intelligence in the intelligence cycle era; that is, the ability to sift information until a "golden nugget" is found or those pieces of limited information that, prima facie, provide objective and data-based evidence of the emerging reality on the other side.[26]

As stated, in the cyber age, intelligence personnel have potential access to infinite information; however, most of the researchers in the majority of the intelligence organizations continue to operate according to traditional practices by "emptying the magazine"; that is, by reading intelligence items based on the collection personnel's prioritization. The establishment of a "social intelligence network,"[27] which also symbolized a new approach to intelligence production, did not change the old habits—at least not in the Military Intelligence Directorate—nor did it create another format of consuming information or developing knowledge. Thus, while intelligence researchers in the civilian environment consume information and develop knowledge according to the digital culture and the "open code,"[28] in the classified intelligence system, they return to consuming information and developing knowledge as if they were still in the 1990s in keeping with the intelligence cycle.

The first handicap that impedes change is conceptual and not technological, since ideas about "webint for every researcher"—the idea that a researcher should be allowed access to the internet and classified databases and the

25 Barger, *Toward a Revolution in Intelligence Affairs*; Michael Warner, "Intelligence in Cyber and Cyber in Intelligence," in *Understanding Cyber Conflict: 14 Analogies*, ed. George Perkovich and Ariel E. Levite (Washington, DC: Georgetown University Press, 2017), pp. 17–31.

26 Bruce Berkowitz, "The Big Difference Between Intelligence and Evidence," *RAND Blog*, February 2003.

27 Kochavi and Ortal, "*Ma'asei Aman*" – Permanent Change in a Changing Reality."

28 Studies show that millennials make their first contact with news via the social media, and only if they are interested in a particular subject do they look for elaboration on regular news channels. See, for example, Roy Greenslade, "How the Different Generations Consume their Daily News," *Guardian*, July 22, 2015.

technological systems that facilitate this—had already emerged in the Israeli intelligence community at the beginning of the 2000s. This conceptual handicap causes intelligence researchers to not fully exploit the nearly infinite potential enjoyed by other researchers, such as in academia or in business.

As noted, the cybersphere enables the creation of a shared intelligence space. In the past, the separation between the collection units, which was based on wave lengths and various production characteristics, is swiftly being replaced by a shared byte-based digital space. In essence, the new collection agent is a technologist, and all of the rest of the intelligence functionaries, whether in collection or research, perform research operations at varying levels and quality and for different needs. The main problem of intelligence in the cyber age is no longer finding the "right" information and its analysis for the purpose of discovering the "secret," but rather asking the right question that creates new knowledge[29] and engages in creating and defining new conceptual categories.[30] This mission is no longer the domain of the researcher alone, just as the ability to locate relevant information and produce it is no longer the domain of only the collection agent; today, both the intelligence collector and researcher have the same basic knowledge and also share similar searching, identifying, and processing capabilities.

The cybersphere creates a shared domain with the adversary, while the intelligence cycle relies, to a great extent, on the geographic boundaries between us and our adversaries.[31] These boundaries enabled the creation of both conceptual and functional separation between research, collection, covert offensive operations, and preventive security; in the cyber age, however, these separations have become artificial and superfluous. A collection operation, which includes accessing a database, is not materially different from a covert

29 A.H., "Does Intelligence Research Need to Change and How?" *Intelligence in Theory and Practice* (Israeli Intelligence Community Commemoration and Heritage Center), no. 2 (2017).

30 Itai Brun, *Intelligence Research: Responsible Practice in an Age of Transformations and Changes* (Israeli Intelligence Community Commemoration and Heritage Center, 2015), pp 58–59 [in Hebrew]. For an elaboration on the creation of new categories and their importance to understanding reality, see Zvi Lanir, *Creating New Categories in the World* (Tel Aviv: Praxis Institute, 2008) [in Hebrew].

31 Robert D. Williams, "(Spy) Game Change: Cyber Networks, Intelligence Collection and Covert Action," *George Washington Law Review* 79, no. 4 (2010): 1162–1200.

offensive operation in cyberspace.[32] The very act of searching for information leaves digital footprints and changes in the web itself. These changes directly impact both the adversary and the side executing the operation, as well as civilians, other rival countries, and friendly nations. Researchers are no longer required nor can they restrict themselves to passive reading of information on the web. Accessing forums requires researchers to assume that they are visible to others, even if using a false identity. This trend greatly challenges the ability to separate between the passive and active intelligence functions, requires the researchers to have sophisticated tools to manage identities on the web, and enables them to become an active partner in the creation and consumption of knowledge on the web.

The cybersphere accelerates the environment's pace of change; the speed at which technologies are replaced, the ease in their dissemination, and their low prices create an infrastructure that allows for enemies, adversaries, friends, the internal intelligence arena, as well as the civilian and business environment to constantly shift. The symbiosis of all these changes creates a reality of constant movement and rapid transformation, which often transpires in an unanticipated, non-linear manner. This pace of change greatly challenges two basic roles of the intelligence cycle. Firstly, it hampers the ability of knowing the right question and thus also the capability of sustaining the "engine" of the intelligence cycle; one side has prioritized clear questions (decision maker or researcher) while the other side has prioritized clear answers (researcher or collector). Secondly, it challenges the ability to preserve the standards of an intelligence product, since the orderly, sequential process of creating information, constructing a stable intelligence picture, and disseminating it is prolonged and often exceeds the time constraints of the rapid events. Furthermore, the cybersphere has changed the kind of expertise required of intelligence personnel; if, in the past, intelligence agents needed expertise only in their specific field of research, in the cyber age, researchers require considerable competence in information technologies, languages, database management, a thorough understanding of networks, statistics and more, in addition to their disciplinary expertise.

32 These understandings led to ideas in the United States of consolidating the Cyber Command with the National Security Agency (NSA). See, for example, Jason Healey, "Shaking Up the Top of Cyber Command," *CIPHER Brief*, October 22, 2017.

The Cybersphere and Intelligence: A Paradigmatic Crisis

In the previous two sections, we presented the changes that the intelligence organizations have implemented in order to sustain the current intelligence cycle paradigm. In the following, we will present a number of examples that characterize the incompatibility of the intelligence work with the cyber age, notwithstanding those changes.

As stated, the intelligence cycle divides intelligence work into collection units and a central research entity. Despite that most of the collection units engage in the cyber era in bytes and the link between them—even before the material reaches the researcher—they continue to work separately, and the connection between them, if it occurs, is done mechanically or by force and does not remove demarcations nor does it become "natural."[33] Interim concepts created in recent years, like "Cyber-HUMINT" (the creation of virtual human entities) and "HUGINT" (combination of HUMINT and SIGINT), or stationing VISINT personnel in the SIGINT unit and vice versa in order to fully exploit the geo-cyber field,[34] convey the complexity of the current situation and the need to re-examine and ascertain whether the existing collection architecture is still valid.

The emergence of cracks in the conceptual walls has destabilized the "barrier" between the intelligence community and its consumers. And indeed, already about a decade ago, the former commander of Unit 8200 called for "demolishing the walls" between his unit—the Intelligence Corps' chief collection unit—and the research agencies.[35] Despite this, the architecture of the intelligence community, both in Israel and elsewhere, has remained unchanged, and the organizational and political barriers continue to determine the pace of the change, in effect, preventing any initiatives for profound changes.

---

33 For elaboration, see Lieut. Col A., "Geographic Intelligence – From a Paper Map to the Geo-Web," in *Challenges of the Intelligence Community in Israel*, ed. Shmuel Even and David Siman-Tov (Tel Aviv: Institute of National Security Studies, 2017); Avi Tal and David Siman-Tov, "HUMINT in the Cybernetic Era – Gaming in Two Worlds," *Military and Strategic Affairs* 7, no. 3 (December 2015): 93–102.

34 Lieut. Col A. V., "A Tactical Technological Body as Bringing Change to the Field Intelligence Deployment," *Intelligence in Theory and Practice* (Israeli Intelligence Community Commemoration and Heritage Center), no. 2 (2017).

35 Siman-Tov and Ofer G., "Intelligence 2.0 – New Approach to the Production of Intelligence."

In the past, the intelligence information production process had been based on an individual's expertise, such as the investigator in HUMINT, the translator or the network intelligence expert in SIGINT, and the expert researcher in that field. The prevailing understanding in the intelligence communities around the world today is that there is a need for cooperation beyond just telephone conversations or exchange of email. As a result, ad hoc entities are formed that rely on cross-organizational team work; however, a significant number of these entities are created as temporary organizations that are dissolved once the mission has been accomplished. Indeed, one can also point to revolutionary attempts, like that of the former director of the CIA, who formed task forces instead of the organization's professional divisions.[36] As a rule, however, the basic architecture that erects a wall between the collection organizations and the research organizations and between the collection organizations inter se prevents the establishment of permanent joint organizations that would also include representatives from outside the intelligence community. This situation is tremendously frustrating for those who are attempting to establish these types of organizations.

Another trend in the discourse is the nature of communications between the research entities in the intelligence communities. Inter alia, at issue is the establishment of organizations that would integrate representatives from all the research entities within the intelligence community,[37] as well as calls for the establishment of a shared research space both in Israel and in the United States. In the mid 2000s, there was an appeal within the Israeli Military Intelligence Directorate to establish an "Intelligence Wikipedia," and similar demands were also voiced in the American intelligence community.[38] Nonetheless, the various research entities in both communities still continue to develop their knowledge separately.

---

36 David Sternberg, "About the Change in the CIA: Task Jointness as an Adaptive Organizational Concept," *Intelligence in Theory and Practice* (Israeli Intelligence Community Commemoration and Heritage Center) no. 1 (2016) [in Hebrew].

37 For information about the term "jointness" and its implementation in military, intelligence and civilian systems, see Kobi Michael and David Siman-Tov, "Jointness in Intelligence Organizations: Theory Put into Practice," *Cyber, Intelligence, and Security* 1, no. 1 (January 2017): 5–30.

38 D. Calvin Andrus, "The Wiki and the Blog: Toward a Complex Adaptive Intelligence Community," *Studies in Intelligence* 49, no. 3 (September 2005): 63–70, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=755904.

An additional trend has been the call to produce shared intelligence products within a framework called "Living Intelligence." The idea was that any intelligence entity could update the product and avoid the endless chain of coordination and redundancies.[39] According to this methodology, the consumer was supposed to receive a "living" integrative product that is constantly updated and at a faster frequency than is customary today. Basically, most of these ideas were not substantively implemented and were apparently ahead of their time, blocked by the traditions of the intelligence communities traditions and their fixed work patterns.

One of the disciplines in which the need for a fundamental change has been felt and discussed for a long time is open-source intelligence.[40] The growing consensus is that open-source intelligence is no longer merely a collection discipline; as a result, the organizational positioning of open-source intelligence is disputed, and two alternatives usually are on the agenda: first, to position open-source intelligence in the collection space; and second, to integrate it in the research space. There is, however, a practical difficulty in implementing these changes. Thus, leaving it in the sphere of collection, at least in Israel, creates quite a few anomalies: the researchers swiftly and fully exploit the information to the point of investigative products even before the collection unit has processed and disseminated the information; the databases available on the web are investigated even before the collection unit has cataloged them; and investigative products and relevant civilian and business information collections are not fully utilized because of a lack of desire to establish a reciprocal relationship on the web.[41]

---

39 David A. Schroeder, "Efficacy and Adoption of Central Web 2.0 and Social Software Tools in U.S. Intelligence Community" (master's thesis, American Military University, March 2011), http://das.doit.wisc.edu/amu/Schroeder_Thesis_MAR11_Redacted.pdf.

40 Hamilton Bean, "The DNI's Open Source Center: An Organizational Communication Perspective," *International Journal of Intelligence and Counterintelligence* 20, no. 2 (February 2007): 240–257; Robert David Steele, "The Open Source Program: Missing in Action," *International Journal of Intelligence and Counterintelligence* 21, no. 3 (May 2008): 609–619.

41 An interesting example of using the open web as a learning space and not only as an information-collection space can be found in *Global Trends*, a periodic publication by the US-based National Intelligence Council (NIC) and in the UK-based Development, Concepts and Doctrine Center (DCDC), which publishes *Global Strategic Trends*. These entities cooperate and consult with experts and with the general public in designated forums, as part of the process of preparing their reports.

From analyzing the trends, it appears that there are flickers of change, but also constraints and obstacles, which are mostly conceptual and organizational. It is possible to identify potential dimensions of change in nearly every intelligence discipline, but the actual transformation is limited in scope. Consequently, we argue that a material change can only take place in the various levels of the internal and external intelligence functioning if a paradigmatic change occurs, and the intelligence community—as the body tasked primarily with the development of knowledge—might miss out on the revolution on this issue taking place in the civilian space.

As stated, among the factors preventing the change are organizational traditions and operational approaches, which are difficult to abandon, and the battles over prestige and resources that such a dramatic change could trigger.[42] Furthermore, many argue that the gradual route that the intelligence community is taking now, which does not jeopardize its existing assets, is preferable. Another key factor hindering change is the absence of a perceived crisis, from both an internal and external perspective. As presented earlier, the change in the American intelligence community occurred after the 9/11 terrorist attacks in the United States and the crisis in Iraq in 2003. In Israel, the intelligence community implemented significant changes following the Agranat Commission's report on the Yom Kippur War. The absence of awareness of a crisis, coupled with a perception of intelligence as being successful—mainly due to its outstanding work with operative and tactical intelligence and its successes with cybernetic intelligence collection—constitute tremendous obstacles that hinder achieving the needed change.

Outline of a New Paradigm: Cybernetic Revolution in Intelligence Affairs

We are currently in a transitional stage from an old paradigm—which is becoming increasingly challenging to sustain—to a new paradigm that has yet to be forged, but nascent inklings of its characteristics are already being implemented in the field. In this section, we will attempt to outline a number of principles of the new paradigm, which we call a Cybernetic Revolution in Intelligence Affairs (CRIA).

42 For a discussion about the issue of battles of prestige and organizational politics, as well as the absence of a sense of crisis in the intelligence community, see Michael and Siman-Tov, "Jointness in Intelligence Organizations."

A constantly changing open system

Itai Brun, the former director of the Research Division in the Military Intelligence Directorate, often stressed that intelligence, and particularly intelligence research, is at the forefront of contending with the uncertainty of the changing reality.[43] This reality, of constant accelerated change, obligates the intelligence community to develop an open approach and structure:

- A culture that encourages a rapid flow of information and knowledge within the intelligence space and between the intelligence space and the civilian space: Studies show that an organization that is less formally organized, less hierarchic, less centralistic, and more decentralized, flexible, and able to delegate authority to lower echelons has a better ability of contending with rapid changes in the environment, adapting, and finding solutions to complex problems.[44]
- Mission structures: The basic architecture of the intelligence community needs to shift from a longitudinal structure based on independent units that are responsible for all the tasks within their purview and the communications between them to a matrix structure, based on multi-disciplinary units that are responsible for a particular problem. Additionally, these mission structures will require maximum latitude to fulfill their needs, and this is done by developing connections with other mission structures and by forming mission-specific structures for necessary secondary tasks. Accordingly, these mission structures will need relative freedom of action to choose the mission and the way to accomplish it. There are two main restrictions to such a structure: the first relates to the need for a centralized management by the organization's directors and middle echelons; to this end, a matrix-style management culture should be developed;[45] the second restriction relates to force-building that will feed these mission structures

43 Brun, *Intelligence Research: Responsible Practice in an Age of Transformations and Changes*, pp. 11–18.

44 P. R. Lawrence and J. W. Lorsch, "Differentiation and Integration in Complex Organizations," *Administrative Science Quarterly* 12, no. 1 (January 1967): 1–47; Henry Mintzberg, *The Structuring of Organizations* (Englewood Cliffs, NJ: Prentice-Hall International, 1979).

45 Lieut. Col. N., "Intelligence Knowledge Community as a Mechanism of Action Providing Strategic and Systemic Flexibility to Aman," *Intelligence in Theory and Practice* (Israeli Intelligence Community Commemoration and Heritage Center) no. 1 (2016): 45–54 [in Hebrew].

and facilitate the continuing development of the basic disciplines. The new collection units that will focus on force-building can consolidate a number of disciplines, such as VISINT and SIGINT or special operations and HUMINT. Such a change could also enable the creation of significant shared spaces between the various intelligence organizations in favor of the force-building.[46]

- Partnership with the civilian, business, and academic sphere: This partnership needs to rely on open discourse and exchanges of information, insights, and assessments. Currently, the connection between the intelligence space and the civilian one is based on a bilateral discourse; whereby the intelligence community receives information and knowledge from external sources, the process is not reciprocal nor synergetic. A partnership between the intelligence and civilian spaces will enable the creation of new intelligence products and exchanges of information and knowledge which, in turn, could lead to fresh thinking about familiar problems, learning about unfamiliar issues, and enhancing the capability to solve various problems and improve existing solutions.

An active system

As we saw, the cybersphere dictates separation from the intelligence cycle paradigm and primarily, separation between active intelligence (which, according to the traditional paradigm, is attributed to collection) and passive intelligence (which is usually attributed to research and processing). A concept, theory, and doctrine need to be developed in which the researcher, in addition to understanding the reality, needs to also be responsible for significant components of intelligence collection (mainly open-source) and processing. This requires the collection units to redefine their role and the research units to provide their researchers with new skills required of "information research officers."[47] The traditional organizational division between some of the collection units and the research units might also change.

46 Yahel Arnon, "Force-buildup in the Intelligence Community in a Changing Reality, *Intelligence in Theory and Practice* (Israeli Intelligence Community Commemoration and Heritage Center), no. 2 (2017).

47 Major (res.) D.G., "The 'Information Research Officer': A New Concept in Intelligence Research," *Intelligence in Theory and Practice* (Israeli Intelligence Community Commemoration and Heritage Center), no. 2 (2017).

A system based on fusion technology, artificial intelligence, and machine learning

These technologies, which national intelligence organizations are only beginning to use (unlike, for example, in business intelligence), are expected to render redundant a significant part of the core intelligence collection and research work according to the intelligence cycle paradigm, especially as it pertains to categorizing information according to spheres of knowledge, interpretations, spheres of interest, and so forth; issuing recommendations for action based on past cases, analogies, and scenarios; and identifying clustering of information.[48] At the same time, a technologies-based system requires new roles to be defined (for example, a researcher of clustering) and new processes (such as quality control in lieu of searching information). This kind of system also renders superfluous the separation between collection and research, since some of the practices of processing and researching also will become technological and automated.

Conclusion

Some of the insights presented in this article are not new. The discourse about the growing gaps between the functioning required of the intelligence communities and their approaches, culture, and structure has existed for more than a decade, both within the American and Israeli intelligence communities. The attempts to generate change and adaptations are also not new. Nevertheless, the intelligence communities have remained loyal to the intelligence cycle paradigm and have failed to generate revolutionary changes. It appears that the main reason for this relates to the absence of a sense of urgency and crisis.

The importance of this article is that it presents clearly and methodically the existing gaps and tensions due to the delay in adopting a new paradigm and indicates that the cyber phenomenon has intensified these gaps and the tensions to the point that the intelligence system can no longer sustain itself in its current format. Concurrently, this article points to the cybersphere as a space that enables the intelligence community to extricate itself from the intelligence cycle paradigm and develop a new paradigm. Processes in this direction are already being partially implemented, even if a complete and total concept has not yet crystallized.

48 Paul Santilli, "Applying Machine Learning to Intelligence Problems," *LinkedIn*.

Clearly, abandoning an old paradigm and adopting a new one before it has been comprehensively designed is not a simple and risk-free process. However, opting to remain rooted in the intelligence cycle paradigm apparently is also not without risks. Moreover, it seems already discernable that hanging onto the old paradigm in the cyber age will quickly lead to major intelligence failures and especially to a failure to fully exploit the enormous potential that the new era offers the intelligence effort.

Developing a Doctrine for Cyberwarfare in the Conventional Campaign

Ron Tira

The cyber realm is in the midst of evolving into another branch of state warfare, similar to ground, naval, air, and space warfare. As such, it is bound to give rise to a concise and mature operational doctrine that will adopt general military patterns and rationales and will be synergistically integrated with other lines of operation in the conventional campaign. Although several cyber superpowers have already developed suitable doctrines and capabilities, most of the world's states are still focused on cybersecurity rather than on offensive and defensive cyberwarfare. Cybersecurity is based on generic products and practices designed to provide security against generic reference threats, which are often sub-state. In contrast, cyberwarfare is conducted against a specific opponent in a particular context, and is based on intelligence concerning the opponent that enables such cyberwarfare.

Keywords: Cyber, Israel, United States, warfare

Toward the Normalization of State Cyberwarfare

The cyber realm is in the process of evolving[1] into another branch of state warfare, similar to ground, naval, air, and space warfare. Thus, it is bound to

Lt. Col. Ron Tira (res.) is a businessperson, who serves as a reservist in Israeli Air Force's Campaign Planning Department. He is co-founder of BlueOcean, a company engaged in cyber capabilities buildup.

1 Amit Sheniak, "Not Merely a Technological Advantage: The United States' Organizational Change in Cyber Warfare," *Cyber, Intelligence, and Security* 1, no. 3 (December 2017): 83–105, http://www.inss.org.il/publication/not-merely-technological-advantage-united-states-organizational-change-cyber-warfare/.

give rise to a concise and mature operational doctrine that will adopt general military patterns and rationales and will be synergistically integrated with other lines of operation in the conventional campaign.

Cyberwarfare is at various stages of evolution in different countries.[2] In some of them, the process is managed in a top-down, orderly, and coherent manner, while in others, development is incremental, resulting from the aggregation of ad-hoc measures, sometimes adopted in response to an urgent need, connecting bottom-up to some overall picture. Some cyber superpowers are in advanced stages of developing a doctrine for cyberwarfare,[3] which is likely to be integrated within the conventional campaign. According to various reports, the world's five leading cyber powers are the United States, Russia, China, the United Kingdom, and Israel.[4]

Cyberwarfare and preparations thereof have taken place mostly covertly, and the open, unclassified sources in this sphere are scarce. The United States provided relatively more information about its cyberwarfare concept in 2010,[5] but most of the unclassified reports concern allocating national resources to cyberspace, determining its organizational structure (such as the National Cybernetic Task Force in Israel),[6] regulation, or information security. These reports deal less with the contents and domain expertise of cyberwarfare doctrine.

---

2 Gabi Siboni and Ofer Assaf, *Guidelines for a National Cyber Strategy*, Memorandum no. 153 (Tel Aviv: Institute for National Security Studies, 2015).

3 US Joint Chiefs of Staff; "Cyberspace Operations," Joint Publication 3-12 (R); US Joint Chiefs of Staff, "Electronic Warfare," Joint Publication 3-13.1; William J. Lynn III, "Defending a New Domain, the Pentagon's Cyber Strategy," *Foreign Affairs* (September/October 2010); Cheryl Pellerin, "Cybercom Chief: Cyberspace Operations Key to Future Warfare," *US Department of Defense*, June 16, 2014; "The Department of Defense Strategy," *US Department of Defense*, April 2015.

4 Keith Breene, "Who are the Cyber Superpowers?," *World Economic Forum*, May 4, 2016.

5 "Cyber Command Fact Sheet," *US Department of Defense*, October 13, 2010.

6 For example, "Advancing the National Capacity in Cyberspace," Israel Government Resolution No. 3611, August 7, 2011, and "Advancing the National Preparedness for Cyber Security," Israel Government Resolution No. 2444, February 15, 2015. See also "Staff Paper for Discussion by the Higher Committee for Science and Technology," July 2013, and "Cyberspace and the Protection of Critical Infrastructure," Knesset Center for Research and Information, May 12, 2013 [in Hebrew], http://www.knesset.gov.il/committees/heb/material/data/mada2013-05-13.doc.

In general, cyberwarfare has not yet matured in most countries.[7] The reasons for this include the following:

- Emphasis is placed on cybersecurity,[8] while the notion of an offensive and defensive campaign in cyberspace is slow to mature;
- A concise and mature doctrine of offensive and defensive cyberwarfare is still lacking;
- Cyber is regarded as an isolated, standalone branch that is not integrated into the conventional campaign;
- The current focus is on cyber in the IT environment (computers and cellular devices accessible from the internet), while insufficient weight is attributed to cyberwarfare in the OT environment[9] (control of operational systems) and cyber directed at weapons systems;[10]
- An emphasis is made on criminal, hacktivist, terrorist, subversive (such as disruption of the democratic process or the capital market), or paramilitary (that is, instances where the attacking state wishes to disavow responsibility for the action) reference threats, while not enough weight is given the superpower/state military reference threats;
- Excessive focus is placed on anecdotes, such as the question of attribution,[11] as if this is the primary characteristic of the cyber field, while assertions are made that the lack of attribution breaks the continuity of Clausewitzian rationale (actually, attribution is not a new or unique issue, as special

7 A similar cybersecurity strategy exists in a large number of countries. To emphasize the point, see the two following examples: German Federal Ministry of the Interior, "Cyber Security Strategy for Germany," February 2011; The Government of Japan, "Cybersecurity Strategy," September 2015.

8 "National Cyber Security Strategies," *European Network and Information Security Agency*, December 2012.

9 Nate Beach-Westmoreland, Jake Styczynski, and Scott Stables, "When The Lights Went Out," *Booz Allen Hamilton*, November 2016.

10 Ltg Larry Wyche, USA Ret. and Mr. Greg Pieratt, "Securing the Army's Weapon Systems and Supply Chain against Cyber Attack," *Institute of Land Warfare*, November 2017.

11 John S. Davis II, Benjamin Adam Boudreaux, Jonathan William Welburn, Jair Aguirre, Cordaye Ogletree, Geoffrey McGovern, and Michael S. Chase, "Stateless Attribution, Toward International Accountability in Cyberspace," *RAND Corporation*, 2017, https://www.rand.org/pubs/research_reports/RR2081.html; Martin C. Libicki, "It Takes More than Offensive Capability to Have an Effective Cyberdeterrence Posture," *RAND Corporation*, 2017, https://www.rand.org/pubs/testimonies/CT465.html.

forces, submarines, and even aircraft are capable of attacking without attribution, without undermining or changing the familiar strategic and campaign patterns). This occurs while inadequate weight is given to the expected normalization of cyberwarfare and its integration within mainstream warfare.

Cyberwarfare is in its initial technological and operational development stages; analogous to the development of military aviation, these stages can be compared to the appearance of biplane observation aircraft in World War I. The potential inherent in the possibility of flying directly toward the enemy's centers of gravity—above the ground defense systems and ground obstacles—was evident, and military leaders, such as Giulio Douhet and Billy Mitchell, formulated the concept of strategic bombing even before the aircraft capable of carrying it out had been developed. Likewise, the doctrine of cyberwarfare must also continue developing vis-à-vis the future potential and serve as a technological and operational compass, even if not all of the tools necessary for fully realizing all of its elements already exist.

Characteristics of Cyberwarfare

As will be made clear in the following pages, cyberwarfare is gradually adopting general military patterns and rationales. As with any branch of warfare, however, cyberwarfare also features its own distinct characteristics that should be evaluated. Cyberwarfare makes it possible to attain control over software, or at least to disrupt its use, and—in the case of software that allows control of a mechanical system—can also cause physical damage to equipment or personnel. When software enables control of a large number of mechanical systems, extensive and even mass physical damage is achievable. Cyberwarfare therefore sometimes enables damage to assets and fatalities, making it at times equivalent to a kinetic attack. Cyberwarfare obviously also makes it possible to disrupt the functioning of software or its data, including those of weapons systems or critical operational systems.

Operating cyber weapons often incurs a low direct operational risk. Under appropriate circumstances, it is therefore possible to confer attractive cost-benefit ratios in comparison with a physical attack, especially in cases in which there is no need for a risky enabling operation for the purpose of creating access to air-gapped networks or of creating access to systems that pose a challenge for remote attack because of technological or operational

considerations. On the other hand, when a cyberattack has not been prepared in advance as part of the pre-conflict routine, it is liable to prove difficult to insert and execute it on short notice in an emergency.

Geographical distance often loses significance in the cyber dimension and it is seemingly possible to attack at any range in cyberspace (at least when it comes to IT systems accessible from the internet or cellular networks). This characteristic extends the range of reference opponents and reference threats on the one hand, while on the other hand, it sometimes constitutes a more comfortable substitute or supplement for a challenging kinetic operation against non-bordering states, while also expanding the possible lines of operation against a coalition of opponents. The strong-weak balance of power in the cyber dimension can be measured separately from other dimensions (as a naval power, for example, might possess a modest land force).

In some cases, the technological or operational challenge of applying a cyber weapon is difficult and requires time; in these cases, it can be assumed that the attacker will try to overcome this challenge before the conflict breaks out ("D-Day minus" operations). The insertion of cyber weapons in the critical systems of potential future opponents could therefore be a pre-conflict routine, which is necessary for effectively launching cyberattacks at a later stage, when a conflict actually has erupted. In other words, in contrast to most branches of warfare, using cyber warfare in a conventional campaign often requires conducting preliminary enabling operations even before a conflict begins. It can be assumed that at least in some cases, exposing an attempt to insert a cyber weapon during pre-conflict routine times will not constitute a casus belli and will not lead to escalation, in contrast to when a military physically enters another country during routine times.

A cyber attacker today and in the foreseeable future will have significant advantage over the defender.[12] The defender must protect a large number of assets, including military platforms and weapons systems; military command and control systems; military communications systems; governmental infrastructure; critical national infrastructure; infrastructure that is non-critical but its disruption would effect morale; commercial corporations of national importance, such as banks and stock exchanges; and the digital civilian

12 *Information Technology and Cyber Operations, Modernization and Policy Issues to Support the Future Force: Hearing before the Subcommittee on Intelligence, Emerging Threats and Capabilities, House of Representatives*, 113th Cong. (2013).

home front in general. The global increase in networking and digitalization processes, which are expected to intensify with the introduction of the Internet of Things (IoT) and the autonomous vehicle, will exponentially both increase the number of assets that can be attacked (or other assets that can be attacked through them) as well as increase accessibility and possible attack vectors. In practice, the attacker can choose from innumerable attack possibilities. In order to penetrate the system that is attacked, the attacker only needs to succeed once in a single attack vector. In contrast, the defender has to successfully defend all the time, all the possible attack vectors leading to his systems.

The attacker also enjoys two other advantages. First, since the defender must defend "everything" while the attacker can focus his efforts wherever he chooses, the manpower required for cyber defense is much greater than in the attack (in contrast to conventional warfare). Thus, the higher quality personnel can be concentrated in the attack, compared to the average personnel in the defense. In cyberwarfare, the quality of the personnel, their talents, creativity, know-how, and proficiency in the latest technological developments, are crucial. In a typical confrontation between an attacker and a defender in a certain attack vector, the attacker (who will assign his best personnel to this attack) assumedly will enjoy an advantage over the defender (who, in the absence of a specific warning, will deploy only average personnel to the relevant attack vector). The second advantage of the attacker, which to some extent results from the first advantage, is that presently, at least, the vulnerability of many systems is much greater than the awareness of the defender to said vulnerabilities. The level of the defender's awareness of the degree of accessibility to his systems is also insufficient, such as the ability to penetrate systems by attacking neighboring systems or third parties in the defender's supply chain.

In cyberwarfare, intelligence gathering is very similar to an attack, to the point of blurring the boundaries between them. In both cases, it is necessary to penetrate the opponent's system and gain control over software. The culmination of the intelligence-gathering process is exfiltrating information, while the end of the attack process is a change or corruption of that same information. The technological and operational process of intelligence gathering and of an attack in cyberwarfare are mostly identical, and it is possible that

the same cyber payload will be used in both intelligence gathering and in an attack, when needed.

As in any other branch of warfare, cyberwarfare is also a consumer of the intelligence needed in order to manage a defensive or offensive campaign. The intelligence necessary for cyberwarfare is not necessarily gathered in the cyber dimension; rather, the most relevant intelligence for conducting a cyberwarfare campaign is sometimes collected through other means, such as human intelligence (HUMINT), communications intelligence (COMINT), and so forth, or is gained through intelligence research using conventional methods.

The Defensive Cyberwarfare Campaign

It is proposed to distinguish between cybersecurity and a defensive campaign in cyberwarfare, based on the following conceptualization and definitions. Cybersecurity is an activity likely to be taken by any party seeking to secure itself in cyberspace, including commercial and private entities. Cybersecurity is based on generic practices and products[13] designed to protect against generic threats. The essence of cybersecurity lies in the securing party (the "blue") focusing on itself, including the way it protects its "fence" (preventing penetration of the blue system by cyber payloads), its routine security behavior (setting honey traps and bait, misleading the attacker by means of deceptive network architecture, or making periodic changes in the blue network's topology), monitoring activity within the blue network, monitoring the information that streams out from the blue network, encryption of the blue network's information, readiness for recovery of the blue network from an attack, and so forth.

In contrast, cyber defense is a campaign conducted by a state or quasi-state entity in order to defend against an attack. Cyber defense is not generic; rather it is conducted in a specific context, against a specific offensive effort by a known or identified attacker. Like any defensive campaign, the essence of cyber defense lies in focusing on the attacker ("red"), while taking a range of operational actions against the efforts carried out by the attacker. When red is preparing for an attack, blue can launch a preemptive attack to prevent the red's attack. After the attack by red has begun, blue can carry

13 "NCSS Good Practice Guide," *European Network and Information Security Agency*, November 2016.

out an interdiction operation, including in communication networks of third countries (often innocent) used by the red.

In cyber defense, as in cybersecurity, blue will also try to prevent red from penetrating its network and will monitor the network in order to detect successful red attacks. At the same time, concrete operational measures can be taken against an identified offensive campaign to thwart the attack. Such measures are not available if blue is only securing its network against generic threats. After detecting a successful red attack within the blue network, the attack payload needs to be uprooted, but in certain cases, there is also room to assess the potential damage and exposure resulting from the attack, contain the attack, and leave it within the blue network, sometimes even while managing a deception operation against it. In some cases, it is better to deal with a familiar and contained attack instead of motivating red to carry out another attack, which might not be detected. In other cases, the appropriate steps would be to carry out a follow-up attack against red in order to disrupt its ability to produce intelligence from the cyber payload that it has used, or to interfere with its ability to deliver commands to that payload.

Conducting such a defense campaign requires intelligence that identifies the attacker; identifies its preparations, intentions, and operational steps; creates a picture of the overall offensive campaign from a range of seemingly isolated operational steps; and analyzes the attacker's technological capabilities and cyber payloads, including the identification of unfamiliar cyber weapons (i.e., a zero-day payload). At the same time, there is a need for tools that can detect attacks that have penetrated the blue network, assess the extent of the potential damage from the penetration, and provide options for containing it.

The Offensive Cyberwarfare Campaign

An offensive cyberwarfare campaign is composed of a number of attacks and enables operations orchestrated under a single strategic rationale. It thereby differs from an isolated attack, which typically characterizes the criminal, hacktivist, or terrorist threats.

The networks and computers of critical systems, both military and national infrastructure, are often air-gapped, and this trend is expected to intensify. Today, the vast majority of cyberattacks take place in the IT environment, which is often accessible to open communications networks (such as the internet). In the future, however, attacks on high-quality and

air-gapped, or otherwise isolated, targets must also be addressed. One of the principal challenges in this type of attack is creating access to the attacked network or computer. In many cases, creating access to an air-gapped target requires an enabling operation that does not take place in cyberspace, such as through the use of special forces, HUMINT, aircraft or naval vessels, and so forth. This point constitutes a key characteristic distinguishing the state or superpower reference threat—in which a state actor is capable of carrying out an enabling operation for creating access—from the sub-state reference threat that will find it difficult in many cases to conduct an enabling operation for establishing access.

An enabling operation for creating access requires regarding the adversary as a "system of systems," an analysis of possible attack vectors, and, of course, executing the enabling operation for creating access. In this framework, it is possible to take advantage of, among other things, vulnerabilities that result from the sub-systems comprising the adversary:

- As in any cyberattack, the architecture of the opponent's computer network, software and encryption vulnerabilities, the options of escalating privileges, failures of the opponent to implement its own security policy, and so forth, should be analyzed.
- In order to create access, the geographic deployment of the rival's computer network and routes of physical access to it should be evaluated. Access can sometimes be created using geographically-proximate networks or local networks upon which the attacked network or its components depend.
- The communications network on which the adversary's computer network operates should be evaluated, and an effort should be made to detect any vulnerabilities, such as segments in which wireless communication is used.
- The feasibility of an attack through the rival's supply chain, i.e., the sources from which he procures its hardware, firmware, and software, should be considered.
- The opponent's interaction with networks and other organizations that are friendly to it, yet have a lower level of security, should be mapped and exploited.

Integration of Cyberwarfare in a Conventional Campaign

The purpose of war is to either force the adversary to accede to our political will, despite his opposition, whether through the threat of force or its use, or

to thwart the opponent's attempt to force us to accede to his political will, whether through the threat of force or its use. The strategy of war might be to achieve military decision by negating the opponent's ability to operate effectively against us in the relevant context, or attrition—exacting a price for war that is not worthwhile in comparison to its goals—or some other strategy relevant to the specific context of war. Such strategy is applied via one or more campaigns. A campaign is a series of actions involving the use of force that have a rational, functional, geographic, synergetic, or other connection between them. The use of force in this context means the use of military means, including non-kinetic means, such as intelligence gathering, electronic warfare, enabling operations (for example, air refueling or operations to resupply ground forces), and so forth. These general military definitions also apply to cyberwarfare.

Cyberwarfare is likely to contribute to the conventional campaign in two ways: First, cyberwarfare can enable the operation of others, such as by disrupting an air defense system, thereby supporting a warplane in performing its mission, or by disrupting the enemy's ground command and control apparatus, thereby making it easier for the blue ground forces to engage the red ones. At the same time, the cyber apparatus might require support by others in order to facilitate its operations, at least in the case of a cyberattack against air-gapped or otherwise isolated systems. Second, cyberwarfare can contribute to the conventional military campaign through directly servings the campaign's or strategy's objective, such as exacting a price of war from the opponent, which will cause it to abandon the war and its political objectives.

It appears that the optimal use of cyberwarfare, at least in certain cases, includes synergy with other branches of warfare in a joint operation. For example, in appropriate cases, an air defense system can be annihilated or suppressed through a combination of fighter jets, attack helicopters, special forces, electronic warfare, and cyberwarfare. In other cases, the opposing country's political will can be attrited and bent through a combination of aerial attacks, naval blockade, and cyberwarfare.

It has been argued that the question of attribution breaks the Clausewitzian linkage between policy and warfare, because if computer networks in a given country "simply" collapse and the event cannot be attributed to a specific player, that same player will find it difficult to achieve his political goals

through cyber means. This is because the attacked state will not identify the attacker, the context, nor the attacker's political will and therefore will be unable to succumb to pressure (as a state might accede to pressure exerted by an overt naval blockade, for example). This argument is incorrect, because many types of warfare—using special operations, submarines, and sometimes even aircraft—are possible without direct tactical attribution. A country under a naval blockade does not have to recognize each rival submarine and understand the tactical circumstances every time one of its merchant ships is sunk in order to comprehend the strategic situation as a whole, while the rival might succeed in forcing his political will on the blockaded country even without being attributed to the sinking of each ship. The same is true of cyberwarfare: cybernetic forensics for every cyber incident is not necessary in order for the attacked state to understand the strategic situation created by the assailant country. In most cases, at least those in a conflict between states, the attacked side does not need to determine attribution through cybernetic forensics in order to assess the situation via conventional intelligence processes and understand the strategic situation.

One question sometimes raised concerns isolating the cyber dimension from other dimensions; for example, if a cyberattack is liable to lead to a kinetic retaliation or only a cyber retaliation, and whether a cyberattack is liable to constitute a casus belli. The answer proposed here is that the same principles applies to cyberwarfare as they do to any other branch of warfare as cyberwarfare is not an isolated and unique branch of warfare. As in any other case, here, too, the decision maker must assess the situation and decide according to the circumstances. A cyberattack against a hospital killing hundreds of people or against a power station that blacks out large parts of a country is no different than a kinetic attack that generates the same effect. The attacked party will assess the situation and react according to the effect generated by the attacker. The attacked is likely to respond using cyber or other means, depending on the circumstances and its relative advantage. If the effect caused by the attacker justifies it, a cyberattack can also constitute a casus belli.

Conclusion: Security Versus a Defensive Campaign

In an analogy to the physical world, if we are to visit a power station, we will almost certainly find fences, watchtowers, CCTV cameras, floodlights,

a number of security vehicles, and a dozen security guards armed with light weapons. The question is for which threat is this an appropriate security solution. The answer is that these means of security are mostly effective against criminal or terrorist threats. This article argues analogously that this is the current development stage of cyber in most countries, except perhaps for the several cyber superpowers.

But what if the threat to this power station is military, such as a raid by a commando battalion, an attack by a strategic bomber, or a submarine launching a cruise missile while loitering two hundred miles away from the power station? In such a case, it is obvious that the power station's security solution is irrelevant. Furthermore, in most cases, an enemy state will not "simply" attack a single power station in and of itself, but that rather would be a part of a campaign that has political and strategic rationale behind it and would involve additional operations. For example, attacking a power station would likely be part of a broader campaign to degrade the national electrical system and other national infrastructure in order to realize a strategy of attrition aimed at enforcing a given policy. It is also likely to include various other enabling operations, such as an enabling attack on the air or naval defense systems before the attack on the electrical system. Defending against such an offensive campaign is conducted in a counter-campaign carried out far from the aforementioned power station and at a far higher intensity than that of its security force. Such a campaign would utilize all means of national power and military might, such as in a preemptive attack against the enemy force or by its interdiction on its way to attacking the electrical system of the defending country. This is analogous to state and high-intensity cyberwarfare.

Most of the world's state and commercial agencies engage in cybersecurity. Cyberwarfare, both defensive and offensive, is still in the early development stages, but it will shape the future.

Cyber Intelligence: In Pursuit of a Better Understanding for an Emerging Practice

Matteo E. Bonfanti

Similar to other cyber-related notions, there is not any crystallized definition of "cyber intelligence," nor are there enough studies focusing on how it is crafted. In light of the above, the present paper draws a clearer picture of this emerging practice by taking stock of the existing analytical work on the topic. The paper reviews the available scientific literature addressing cyber intelligence, discusses the notion of cyber INT, and examines how this intelligence is crafted through the lens of the (cyber) "intelligence cycle." The paper concludes by stressing the importance of developing a clear and shared understanding of cyber intelligence among relevant security and, especially, cybersecurity stakeholders.

Keywords: Cybersecurity, intelligence, cyber intelligence, cyber intelligence process, notion, models

Introduction

Over the last decade, there has been a growing push toward adopting intelligence-led approaches/solutions to deal with cyber threats. The push has come from several members of the (not-formalized) international cybersecurity community that consists of representatives from supranational institutions and agencies, domestic public bodies, private organizations, and academia. They have, for instance, sponsored the adoption of ad hoc concepts and solutions for the delivery of "cyber threat information/intelligence" (CTI), a product that provides its consumers with the (technical) understanding

Dr. Matteo E. Bonfanti is senior researcher at the ETH Center for Security Studies, Zurich.

of malicious networks operations and activities and enables them to take subsequent actions.[1] However, CTI alone does not prove to be fully suitable for supporting advanced prevention of cyberthreats.[2] This is due to the technical nature and strictly operational scope of cyber threat information/intelligence that allows its consumers to understand network events and trends ("inside the wire perspective") and adopt reactive measures. Generally, CTI products are not built and do not provide knowledge on the wider and articulated context within which cyber threats are framed.[3] They do not grant the understanding of cyber threat ecosystems nor do they enable advanced prediction/prevention.

By endorsing the idea that organizations should move from reactive to proactive security management postures and opposing the attitude to interpret cybersecurity mostly as "measures taken after-the-event" and "static perimeter defense," different representatives of the cybersecurity community are now sponsoring the adoption of concepts, tools, and practices for the crafting and sharing of all-encompassing intelligence about cyber threats.[4] This intelligence should enable its consumers to comprehend the operational, tactical, and strategic contexts of the threats (agents, capabilities, motivations, goals, impact, and consequences not only from a technical perspective), foresee their developments in the short, mid, and long terms, and take informed decisions on preventive actions to be taken. If integrated in their security-related decision-making processes, it should enable organizations to assume

1 Sharing of threat information, current attack patterns, software vulnerabilities and so forth have been standardized in process through the establishment of a network of CSIRTs (Computer Security Incident Response Teams). They have been augmented by the establishment and development of a number of initiatives, such as STIX/TAXII, CyBox, MISPs (Malware Information Sharing Platform). See, for example, http://stixproject.github.io/supporters/.

2 Brian P. Kime, "Threat Intelligence: Planning and Direction," *SANS Institute InfoSec Reading Room* (2017), p. 3, https://www.sans.org/reading-room/whitepapers/threatintelligence/threat-intelligence-planning-direction-36857. As stressed by the author, Indicators of Compromise (IOCs), like virus signatures and IP addresses, hashes of malware files or URLs or domain names of botnet command and control servers are not by themselves intelligence. They are information useful for network static defense.

3 See Michael Montecillo, "Why Context is King," *Security Intelligence*, April 22, 2014, https://securityintelligence.com/enterprise-it-security-context-king/.

4 The term "proactive" should be here understood as the capacity to address actual potential cyber threats by strengthening defense and response measures.

"predictive and anticipatory rather than past-oriented," "dynamic than static," and "agile and quick adaptable than rigid and conformed" postures toward cyber-related perils. The above-described intelligence is often labeled "cyber intelligence" (cyber INT or CYBINT) to differentiate it from the technically interpreted and narrow scope "cyber threat information/intelligence." In general, cyber intelligence is used to convey the idea of widely scoped and better qualified knowledge of actual or potential events regarding cyberspace that may endanger an organization.[5]

Similar to many other cyber-related notions, there is neither a crystallized definition nor a real common understanding of cyber intelligence—as a product and/or process—among policy makers, practitioner organizations, scholars, and public opinion. If one looks at the relevant policies or mechanisms that have been recently implemented (especially across Europe) as well as other documentation issued by private or public organizations and the academia, cyber intelligence is not always comprehensively defined and definitions vary.[6] Despite the growing use of this or similar expressions by the media as well as scholars and practitioners (especially by cybersecurity vendors for marketing reasons), current thinking on the subject is limited and not well developed. This holds especially true if one looks at the academic or other intellectual works on the topic that have been so far produced in Europe.[7] A deeper investigation of the subject—both from a theoretical and practical standpoint—is missing. On the contrary, the academic and practitioners' reflections on cyber intelligence are relatively more advanced among the

5 See also below.

6 Matteo E. Bonfanti, "Another –INT on the Horizon? Cyber intelligence is the New Black," paper presented at the Intelligence in the Knowledge Society Conference, Bucharest, October 26–27, 2017. An anthology of presented papers will be published in 2018.

7 At least this seems to be the case in some of the literature reviewed for the purpose of writing this paper. See, for example, Mario Caligiuri, *Cyber Intelligence. Tra libertà e sicurezza* (Roma: Donzelli, 2016); Mario Caliguiri, "Cyber Intelligence, la Sfida dei Data Scientist," June 2016, https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/cyber cyber intelligence-la-sfida-dei-data-scientist.html; Antonio Teti, "Cyber Intelligence e Cyber Espionage. Come Cambiano i Servizi di Intelligence nell'Era del Cyber Spazio," *Gnosis. Rivista Italiana d'Intelligence* 3 (2013): 95–121; Umberto Gori and Luigi S. Germani, *Information Warfare 2011. La sfida della Cyber Intelligence al sistema Italia* (Bologna: Franco Angeli 2012).

US security and cybersecurity stakeholders.[8] This could be the consequence of the earlier adoption of cyber intelligence-related concepts, practices, and technological solutions by US-based organizations.[9] However, given that the push toward the adoption of cyber intelligence programs seems to be on the rise also among non-US cybersecurity stakeholders, it is worth expanding the discussion on this topic. In particular, it may be valuable to examine the notion of cyber intelligence in more detail as well as understand the implications arising from the employment of cyber INT-led approaches, methodologies, tools, and cooperation frameworks by national agencies and organizations.

The present paper intends to provide a targeted contribution to the debate on cyber intelligence. It tries to draw a clearer picture of this emerging practice by taking stock of the existing analytical works on the topic. The paper reviews the available scientific literature addressing cyber intelligence, discusses the notion of cyber intelligence, and examines how it is crafted through the lens of the (cyber) "intelligence cycle." The paper concludes by stressing the need for a clear and shared understanding of cyber intelligence among relevant security and, especially, cybersecurity stakeholders.[10]

---

8 In addition to the literature that is cited below, see also discussion held by US cybersecurity stakeholders on the Cyber Intelligence Blog at https://cyberintelblog.wordpress.com/.

9 See, for example, Office of the Director of National Intelligence, "The National Intelligence Strategy of the United States of America," 2014, https://www.dni.gov/files/documents/2014_NIS_Publication.pdf. The strategy defines cyber intelligence as follows: "the collection, processing, analysis, and dissemination of information from all sources of intelligence on foreign actors' cyber programs, intentions, capabilities, research and development, tactics, and operational activities and indicators; their impact or potential effects on national security, information systems, infrastructure, and data; and network characterization, or insight into the components, structures, use, and vulnerabilities of foreign information systems." Ibid., p. 8. See also US Department of Defense Science Board, "Resilient military systems and the advanced cyber threat," January 2013, pp. 46 and 49, http://www.dtic.mil/docs/citations/ADA569975; US Department of Defense Science Board, "The Department of Defense Cyber Strategy," April, 2015, p. 24, https://www.defense.gov/Portals/1/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

10 The paper is based on preliminary research that is currently carried out as part of a three-year research project defined and run by the author.

On Terminology and (Shared) Notions

In everyday language, "cyber intelligence" is mainly used as an enveloping and catch-all expression. What is cyber intelligence more exactly? As a product and a process, is it intelligence "from," "on," "within" or "for" cyberspace or some combination thereof? To what extent does it focus on this space or cover events/phenomena occurring in the physical domain? What are the main sources of cyber INT? How is it crafted? Is the "traditional" intelligence cycle applicable to cyber intelligence? What are the issues associated with the crafting and sharing of cyber intelligence? Answering to these framework or other more specific questions is not trivial.

For instance, the lack of a uniform understanding of the term "cyber" hinders any attempt to come up with a comprehensive and uniform notion of cyber intelligence. Indeed, whereas it is more or less undisputed establishing what intelligence (as product and process) is, defining it in relation to the cyber domain is challenging. In general, reflections on cyber intelligence employ concepts, frameworks, and terminology derived from the intelligence community and adopt/adapt them to cyberspace.[11] This seems to be a logical approach given that some concepts are already established and there is no need to "re-invent the wheel." One may wonder, however, to what extent these concepts are applicable to a domain that differs from the traditionally known domains. Cyber is, in fact, a man-made, highly evolving, technologically shaped, and not fully tangible environment, which, perhaps, needs to be interpreted through different paradigms. Its interactions with the physical/real domain are yet to be fully understood.

Furthermore, cyber intelligence is a relatively new practice, which is far from being fully tested, assessed, and developed. There is not enough shared experience on how it works and on the best capabilities to carry it out effectively. This hampers any attempt to come up with a thorough interpretative model for cyber INT.

The above considerations are important. They should not be disregarded by anyone who tried to adopt a less biased or uncertain approach to the study

11 Robert M. Lee, "An Introduction to Cyber Intelligence," (blog) *Tripwire*, January 16, 2014, https://www.tripwire.com/state-of-security/security-data-protection/introduction-cyber cyber intelligence/; Stephanie Helm, "Intelligence, Cyberspace and National Security," paper given at EMC Chair Symposium.

of cyber intelligence. They help in explaining why there is not yet an agreed and crystallized definition of cyber intelligence.

Cyber Intelligence: Actionable Knowledge "From" or "For" Cyber?

Depending on the scope of the information-gathering activities, the means employed to carry them out and the final purpose they serve, there are actually two ways of looking at or interpreting cyber intelligence.[12] One way is to think about cyber INT as intelligence "from" cyber; that is, knowledge produced through the analysis of any valuable information collected "within" or "through" cyberspace. This is the cyber intelligence stricto sensu. From this perspective, "cyber" refers to both the domain where data are sourced or—in other words— that vast digital repository of information amenable to be retrieved and processed; and the tools/techniques/media through which these data are collected (for example, via Computer Network Exploitation technologies and techniques).[13] According to this interpretation, cyber INT can, in principle, support decision making in any domain and not only to counter cyber threats. It can support a broad variety of missions in government, industry, and academia, including policy making, strategic planning, international negotiations, risk management, and strategic communication in areas beyond cybersecurity.[14] In other words, cyber intelligence may operate "independently and does not necessarily need to support a cybersecurity mission."[15] However, given that cyber intelligence is often discussed in relation to cybersecurity or the prevention of and response to cyber threats, these are the primary—but, again, not exclusive—goals of this type of intelligence.

12 Matthew M. Hurley, "For and From Cyberspace Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance," *Air & Space Power Journal* 26, no. 6 (2012): 12–33.

13 Ross W. Bellaby, "Justifying Cyber-Intelligence?" *Journal of Military Ethics* 15, no. 4 (2016): 299–319; Hurley, "For and From Cyberspace," p. 13. Computer Network Exploitation or cyber exploitation refers to the secret collection and reproduction of digital data from computers or networks.

14 Troy Townsend, Melissa K. Ludwick, Jay McAllister, Andrew O. Mellinger, and Kate A. Sereno, "SEI Innovation Center Report: Cyber Intelligence Tradecraft Project: Summary of Key Findings," (January 2013), pp. 2.01–2.20, spec. 2.5, https://resources.sei.cmu.edu/asset_files/WhitePaper/2013_019_001_40212.pdf.

15 Ibid.

Another way to interpret cyber INT is considering it as intelligence "for" cyber; that is, insight that is derived from an all-source intelligence activity occurring within and outside cyberspace. It is cyber intelligence lato sensu. In this sense, the intelligence "for" cyber can also include (or be built on) intelligence "from" cyber. It can draw from any intelligence discipline that supplies crucial knowledge, regardless of the source, method, or medium employed for crafting it. As such, cyber intelligence may therefore result from the combination of Open Source Intelligence (OSINT), Signal Intelligence (SIGINT), Geospatial Intelligence (GEOINT), Social Media Intelligence (SOCMINT), and Human Intelligence (HUMINT).[16] From this point of view, cyber intelligence is less a discipline itself than an analytic practice relying on information/intelligence collected also through other disciplines and intended to inform decision makers on issues pertaining to activities in the cyber domain.[17] What qualifies this kind of intelligence as "cyber " is the purpose for which it is crafted: to support decision making on cyberspace-related issues.

The two discussed perspectives on cyber intelligence—intelligence "from" and "for" cyber—are often condensed into one single comprehensive concept. This is also due to the fact that intelligence "for" cyber actually incorporates the one "from" cyber. The result is a broader notion of cyber intelligence that includes the collection, processing, evaluation, analysis, integration, and interpretation of information that is available "within," "through," and/or "outside" cyberspace to enhance decision making on cyber-related menaces.

It is worth noting, however, that when looking at the "traditional" intelligence disciplines encompassed by the notion of cyber intelligence

16 Aaron F. Brantly, *The Decision to Attack: Military and Intelligence Cyber Decision Making* (Athens GA: University of Georgia Press, 2016), Ch. 7, pp. 103–108 and 116–121.

17 Intelligence and National Security Alliance, "Operational Levels of Cyber Intelligence," September 2013, pp. 1–14, https://www.insaonline.org/operational-levels-of-cyber cyber intelligence/. See also Intelligence and National Security Alliance, "Cyber Intelligence: Setting the Landscape for an Emerging Discipline," September 2011, pp. 1–20, https://www.insaonline.org/cyber cyber intelligence-setting-the-landscape-for-an-emerging-discipline/. On the existing intelligence disciplines, see, among others, the UK Ministry of Defence, "Understanding and Intelligence Support to Joint Operations," Joint Doctrine Publication 2-00, August 2011, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/311572/20110830_jdp2_00_ed3_with_change1.pdf.

lato sensu, their narrower and circumscribed projection on cyberspace has determined the development of ad hoc concepts and approaches often referred as virtual HUMINT, virtual or internet-based OSINT, virtual COMINT, and so forth. The adjective "virtual" indicates that intelligence activities are carried out within the cyberspace or through computer-generated tools. The association of "virtual" with "traditional" INT concepts/practices refers to the adoption of methods/approaches/tools that are employed by these latter practices and adapted for cyberspace.[18] A bit different from the above concepts is the notion of SOCMINT. According to some scholars/practitioners, SOCMINT is as a stand-alone discipline that has specific features.[19]

As for the information for crafting cyber intelligence, this may range from network technical data (for example, hardware and software data), data on hostile organizations and their capabilities, ongoing cyber activities, to potentially any relevant data on geopolitical events.[20] The type of data as well as its classification are not functional to the definition of cyber intelligence. Data can be raw or already processed information; it can be obtained legally or through unlawful intrusion/exploitation actions from open, proprietary, or other classified sources.[21] As the literature suggests, multiple sources of information are needed to develop a more holistic understanding of the threat environment and to produce a comprehensive cyber INT.[22] The most important aspect of the data is that it should be somehow validated. When analyzed, information should allow decision makers to identify, track, and predict cyber capabilities, intentions, and activities that offer courses of

18 For example, the virtual HUMINT approach aims at collecting tactical/operational intelligence from the information generated by members of virtual communities.

19 David Omand, Jamie Bartlett, and Carl Miller, *#Intelligence* (London: Demos Publishing, 2012). See also, Matteo E. Bonfanti, "Social Media Intelligence a Salvaguardia dell'Interesse Nazionale. Limiti e Opportunità di una Pratica da Sviluppare," in *Intelligence e Interesse Nazionale*, ed. Umberto Gori and Luigi Martino (Rome: Aracne, 2015), pp. 231–262.

20 Jung-ho Eom, "Roles and Responsibilities of Cyber Intelligence for Cyber Operations in Cyberspace," *International Journal of Software Engineering and Its Applications* 8, no. 9 (2014): 137–146. This article deals with cyber intelligence for military purposes.

21 Robert M. Lee, "Cyber Intelligence Collection Operations," 2014, https://www.tripwire.com/state-of-security/security-data-protection/cyber cyber intelligence-collection-operations/.

22 Intelligence and National Security Alliance, "Cyber Intelligence," p. 1.

action.[23] This is the main feature of cyber intelligence; that is, the enabling goal of providing its consumers with insight into potentially hostile activities that may occur in the cyber domain or may be perpetrated through or against cyberspace, allowing them to design effective preventive (proactive) or counteractive (reactive) measures.

Depending on its scope or level of actionability, cyber intelligence can be strategic, tactical, or operational.[24] There is no uniform interpretation of what the different levels of cyber INT should consist. According to the available literature, strategic cyber INT focuses on the long term. Typically, it reviews trends in current and emerging threats and examines opportunities to contain these threats. It serves apical decision-making processes aimed at achieving an organization's mission and determining its direction and objectives. Strategic cyber INT covers the threat landscape for macro trends (political, social, and economic) affecting the organization and identifies the threat actors, their goals, and how they may attempt to achieve them; it is rich in contextual information.[25] Tactical cyber intelligence concerns what happens on the network. It also examines the strength and vulnerabilities of an organization, and the tactics, techniques, and procedures (TTPs) employed by the threat actors.[26] Due to its nature and reach, tactical cyber INT corresponds generally to cyber threat intelligence.[27] Generally more technical in nature, it informs the specific network-centered steps and actions the organization can take to protect assets, maintain continuity, and restore operations. As far as operational cyber INT is concerned, it consists of knowledge of imminent or direct threats to an organization. It enables and

23 Townsend et al., "SEI Innovation Center Report."

24 See for example, Randy Borum, "Getting 'Left of the Hack': Honing Your Cyber Intelligence Can Thwart Intruders," InfoSecurity Professional (September/October 2014), https://works.bepress.com/randy_borum/63/.

25 Randy Borum, John Felker, Sean Kern, Kristen Dennesen, and Tonya Feyes, "Strategic Cyber Intelligence," *Information & Computer Security* 23, no. 3 (2015): 317–332. See also, Intelligence and National Security Alliance, "Strategic Cyber Intelligence," March, 2014, pp. 1–16, https://www.insaonline.org/strategic-cyber cyber intelligence/.

26 Intelligence and National Security Alliance, "Tactical Cyber Intelligence," December, 2015, pp. 1–16, https://www.insaonline.org/tactical-cyber cyber intelligence/.

27 Ibid.

sustains day-to-day operations and output. At this level, cyber intelligence looks at the organization's internal processes and vulnerabilities.[28]

It is worth repeating that the described distinction between the levels of cyber INT is mainly scholastic. In practice, there is no clear demarcation from one level of intelligence to another; they frequently overlap or are combined. Furthermore, the meaning of strategic, tactical, and operational is likely to vary across organizations because of their size, complexity, mission, and related attributes.[29] Regardless of any clear-cut demarcation between the levels, the capacity of an organization to consider all these levels and craft intelligence that allows it to understand the challenges and opportunities it is likely to encounter in the short-mid-long terms is quite important. As a finished product, it seems there are no established formats or standards for presenting cyber intelligence to decision makers.

The Cyber Intelligence Process: Alternative vs. Traditional Models

Just like in the case of other intelligence products/disciplines, cyber intelligence is crafted through a set of activities/functions. Traditionally, this set of activities/functions is represented and explained through the "intelligence cycle" model.[30] The model has been studied and questioned several times by practitioners and academics to the point that alternative models have

28 Intelligence and National Strategic Alliance "Operational Cyber Intelligence," October, 2015, pp. 1–16, https://www.insaonline.org/operational-cyber cyber intelligence/.

29 Intelligence and National Strategic Alliance, "Strategic Cyber Intelligence," p. 4.

30 While there are different representations of the intelligence cycle, the most common comprises five distinct functions: Planning and Direction, Collection, Processing, Analysis, and Dissemination. Some of these functions may be further broken down, thus making the overall cycle consisting of Planning and Direction, Collection, Collation, Evaluation, Analysis, Integration, Interpretation, and Dissemination. On the intelligence cycle, see Mark Phythian, ed. *Understanding the Intelligence Cycle* (London and New York: Routledge, 2013). In particular, see Philip H.J. Davies, Kristian Gustafson, and Ian Ridgen, "The Intelligence Cycle is Dead, Long Live the Intelligence Cycle," in *Understanding the Intelligence Cycle*, p. 56.

been proposed and discussed.[31] The "validity/applicability" of the traditional intelligence cycle is also questioned in the context of cyber intelligence. As one eminent expert noted, "as intelligence grows ever more digitalised and 'cyberised' (in its subject matter, its methods, and its forms), a clearer understanding that the Intelligence Cycle is actually quite a dated heuristic device—rather than a constructive dimension of intelligence as such—can liberate *stakeholders* to think about intelligence in more innovative ways."[32] This view is shared by other scholars and experts. They stress the limited applicability of the model to intelligence generated "from" and "for" cyber; they underline its inability to represent and explain the crafting process of cyber intelligence. Meant as a linear and reiterative cycle, the traditional model does not emphasize the inter-related nature of the activities (planning, collection, processing, and so forth) that the cyber intelligence process consists of and their mutual relevance; in other words, it does not capture their inter-dependencies and mutual influences.

Actually, the above critics draw from arguments that are made for describing the inadequate representativeness of the intelligence cycle in general, regardless of the specific INT discipline at stake.[33] Therefore, one may question more in-depth if and why an ad hoc interpretative model is necessary to explain the cyber intelligence process; or, in other words, if and why the cyber INT process is so peculiar and different from the processes embedded in other INT disciplines that it requires being described through an alternative model. Providing consistent answers to the above questions would require a clear, comprehensive, and thorough understanding of cyber INT as a concept and, above all, as a practice. Such an understanding is difficult to reach due to the lack of enough reflections and experience in cyber INT. Therefore, at the current stage, the definition of an interpretative model

31 On the flaws of the traditional intelligence cycle in representing any intelligence process, see the different contributions in Phythian, ed. *Understanding the Intelligence Cycle*. It is worth noting that all models lack accuracy because they are simplifications of complex realities. Furthermore, models are not processes; rather, they are reduced representations of processes. Therefore, it does not makes sense to expect from the intelligence cycle model—as well as any other potential model—to provide an holistic, all-encompassing, and fully detailed representation of the intelligence process. Such models would be incredibly complex and have low practical value.

32 Michael Warner, "The Past and Future of the Intelligence Cycle," in *Understanding the Intelligence Cycle*, p. 19.

33 Phythian, ed. *Understanding the Intelligence Cycle*.

represents mostly a sort of intellectual exercise or a test whose results should be progressively validated. Nonetheless, some arguments seem to support well the definition of an ad hoc model to explain the cyber INT process.

Tautologically speaking, the main feature of cyber INT lies in the fact that it is "cyber centered"; that is, it is knowledge concerning cyber-related issues. Cyber INT involves the analysis of information collected from cyberspace as well as from other sources for achieving cyber-related purposes. At the very basic level, the adjective "cyber" refers to a man-made, highly evolving, technologically shaped and not fully tangible domain.[34] In this domain, information is generated, processed, disseminated, shared, stored, altered, consumed, and destroyed by a multitude of actors at an incredible speed.[35] The impact of targeted decision making on cyber-related issues and its effects on both the virtual and physical domains are difficult to foresee. This affects the way in which cyber intelligence is crafted and consumed. It challenges the core functions of the intelligence process when applied to the cybersphere, namely, the collection, evaluation, analysis, integration, interpretation of information, and dissemination of intelligence.

With regard to the collection and evaluation, cyber intelligence relies also on information delivered by uncontrolled sources, such as the internet.[36] This information should be filtered, evaluated, and (somehow) validated. Filtering is paramount in order to select only significant items of information from cyberspace. Evaluation is often a challenging task due to the high volatility, anonymity, and uncertainty of data available in cyberspace and

34 This domain is both an element and the result of the digital revolution. See Luciano Floridi, *Information: A Very Short Introduction* (Oxford: Oxford University Press; 2010); Luciano Floridi, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality* (Oxford: Oxford University Press, 2016).

35 Warner, "Past and Future of the Intelligence Cycle," p. 16.

36 Collection can be defined as the exploitation of sources and the delivery of the information obtained for processing and analysis. A source can be a person, object, process, or system from which information can be obtained. Sources are uncontrolled when they are not under formal supervision and direction of an organization. One may think of information generated by internet users or other actors in cyberspace. Evaluation can be defined as a phase in the analysis function that constitute the appraisal of an information in respect of the reliability of the source and the credibility of the information. See, for example, the UK Ministry of Defence, "Understanding and Intelligence Support to Joint Operations," Joint Doctrine Publication 2-00, August, 2011, pp. 3-14 and 3-20, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/311572/20110830_jdp2_00_ed3_with_change1.pdf.

the heterogeneity of data sources. To validate data, it becomes therefore paramount to corroborate the information derived from one source with that derived from other sources, and it is better if at least one of the former is controlled. Filtering, evaluation, and validation aim at mitigating the so-called "information anarchy" generated by the increasing volume of available data coupled with the lack of control over them. Given that the crafting process of cyber intelligence may also draw on information/intelligence produced through other disciplines, the integration of all relevant pieces of knowledge into one single and consistent product can be challenging. This is due to the different format, nature, and grade of uncertainty of information and intelligence obtained from cyberspace (for example, information or other technical data sourced from social media, web forums, and so forth) confronted with other "non-virtual" sources.[37] The grade of uncertainty affects also the interpretation of processed information; that is, the judgment and deductions based on it, which are generally added in the final cyber INT product. Such uncertainty should also be clearly conveyed to the consumer of cyber intelligence, who should be aware of its main limits in terms of accuracy.

Another relevant aspect to be considered when defining any interpretative model for the cyber INT process is the tight time frame that often is required for executing intelligence functions. This demands that functions occur simultaneously or that shortcuts are taken in their execution. In other words, functions do not run in a circle but establish an "all-channel network" among themselves.[38]

The above-discussed requirements of the cyber INT crafting process—and the challenges they pose—seem to prompt the definition of a specific interpretative model that could better capture the peculiarities of the process. By looking at the literature, a team of experts and academics working at the Software and Engineering Institute (SEI) of the Carnegie Mellon University proposed their own model a couple of years ago.[39] The SEI model differs from the traditional intelligence cycle because of the adopted terminology, the non-linear and strictly consequential logic of the functions the process

37 Integration can be defined as the function on the intelligence process whereby analyzed information and /or intelligence is selected and combined into a pattern in the course of the production of further intelligence. Ibid. p. 3–22

38 See, for example, Philip H.J. Davies, Kristian Gustafson, and Ian Ridgen, "The Intelligence Cycle is Dead, Long Live the Intelligence Cycle," p. 64 ff.

39 Townsend et al., "SEI Innovation Center Report."

consists of, the breakdown of the analysis function into two specialized functions (the technical or functional analysis and the strategic analysis), and the capacity to capture both the "narrow" technical cybersecurity and the "wider" cyber threats-prevention purposes that cyber intelligence can serve within an organization. As it is represented, the proposed model accommodates the interpretation of cyber intelligence as an analytic practice relying on information/intelligence collected also through other disciplines and that is intended to inform decision makers on issues pertaining to activities in the cyber domain.[40] The SEI model consists of five functions: (1) the determination of the "environment" that establishes the scope of the cyber intelligence effort and influences what information is needed to accomplish it;[41] (2) the "data gathering" or the exploration of data sources and collection and filtering of information through automated and labor-intensive tools;[42] (3) the "functional analysis," which is the performance of technical and tailored analysis (typically in support of a cybersecurity mission) aimed at deriving the "what" and "how" of cyber threats;[43] (4) the "strategic analysis" entailing the review, integration with contextual information, and further elaboration of the functional cyber intelligence with the goal of answering

40 Ibid.

41 Ibid., p. 2.9. Environment is meant as both internal and external. The determination of the internal environment includes the studying of an organization's global cyber presence, the infrastructure that is accessible through the internet, as well as the definition of what data needs to be collected to maintain network situational awareness. Externally, the determination of the environment requires to know which entities are capable of affecting organizations' networks. It must find out and map system vulnerabilities, intrusion or network attack vectors, the tactics, techniques, procedures, and tools used by relevant threat actors. As it is suggested in Townsend et al., "By investing the time and energy to define the environment, organizations significantly improved their data gathering efforts, resulting in more efficient and effective cyber intelligence programs."

42 Ibid., p. 2.11. Data gathering should cover both internal (net-flow, logs, user demographics) and external sources (third-party intelligence providers, open source news, social media). It should focus on the pertinent threats and strategic needs identified while learning about their organization's environment. Indeed, effective data gathering should be based on the definition of the environment. It should target the necessary data for conducting meaningful analysis on critical cyber threats.

43 Ibid., p. 2.13. This function includes the verification/validation of data based on the quality of the source, reporting history, and independent verification of corroborating sources.

the "who" and "why" questions;[44] and (5) the "reporting and feedback"; that is, the dissemination of cyber intelligence to decision makers and the collection of feedback.[45]

The main dependencies and mutual influences among the described functions are the following: Data gathering should be premised upon the determination of the environment, which is itself influenced by the decisions taken by the organization on the basis of cyber intelligence consumed. The intelligence resulting from the functional analysis can inform decisions on actions to be taken at the technical-network level of an organization which, in turn, impact on the determination of the internal environment; the same goes for intelligence resulting from the strategic function, which affects both the internal and external environment. The strategic function also renders the intelligence resulting from the functional analysis more consumable by apical decision makers who may not have a technical background. From this perspective, it is a sort of add-on application that contributes in bridging the communication gap between analysts and top decision makers. The latter provide feedback on the intelligence received in order to shape analytical functions, adjust the direction of the organization, and therefore influence the environment.

Questioning the "validity" of the SEI model is beyond the scope of this paper. The model was designed and proposed as a result of empirical work that mapped and assessed current practices in US cyber intelligence. It is grounded in data and represents the state of the art within selected US-based organizations. It has also a normative reach; that is, it suggests how the process should work to be effective. Furthermore, the proposed model has the advantage of being relatively simple while, at the same time, representative of practices adopted by different types of organizations, such as small corporations, larger industries, and governmental agencies. However, its representativeness is likely to fade away at both the lower and higher levels—the individual and multi-partnership or transnational levels—of

44 Ibid., 2.15. Strategic analysis adds perspective, context, and depth to functional analysis. It is ultimately rooted in technical data but incorporates information outside traditional technical feeds. The resulting strategic analysis populated threat actor profiles, provided global situational awareness, and informed decision makers of the strategic implications cyber threats posed to organizations, industries, economies, and countries.

45 Ibid., p. 2.17.

occurrence of the cyber intelligence process. Especially at the latter level, the degree of organizational/institutional complexity will probably render the intelligence model unfit. In addition, technological developments in the field of cyber will probably affect the model and require further (periodical) re-elaborations.[46] Lastly, the proposed model still suggests that collection and analysis are sequential; that is, the latter can only begin once the former is complete. In practice, the two functions are interactive and occur concurrently. That being said, one may acknowledge that the SEI proposed model represents a sound and initial attempt to better explain how cyber intelligence is and should be crafted.[47]

Conclusion

Having a clear understanding of cyber INT is important. It can help relevant stakeholders to be consistent when they promote programs or take actions concerning cyber intelligence at the policy, legal, operational, and other levels. Such understanding should be premised upon the definition of a sound conceptual framework of cyber intelligence. This framework should serve as a structure to be employed for making conceptual distinctions, organizing ideas, and interlinking them to provide a comprehensive understanding of cyber intelligence. The adoption of such a framework would also represent a paramount element to develop cyber INT as a discipline; that is, a specific area of study or work in intelligence. Although most of the literature considers cyber INT as being an already-established or soon-to-be-established discipline, it does not seem to be the case. The lack of a more mature theoretical elaboration of cyber INT, coupled with the relatively limited experience in it, makes it difficult to consider this type of intelligence as a recognized area or branch of intelligence. In other words, cyber INT should not be considered a discipline because it has not yet been sufficiently theoretically defined nor practiced. Furthermore, as described above, the nature of cyber INT and its crafting process makes it less a discipline than an analytic practice, which relies on information/intelligence collected also through other disciplines. Of

46 This is actually acknowledged by the promoters of this model when discussing about analytical capabilities "because technology changes so quickly, the process of producing cyber intelligence analysis had to be dynamic enough to capture rapidly evolving tools, capabilities, and sophistication of adversaries."

47 A deeper discussion of the cyber intelligence process as well as the formulation on another alternative interpretative model will be carried out within the research project.

course, nothing prevents cyber INT from establishing itself as a discipline that employs specific technical or human resources throughout the different functions of its crafting process.

Finally, a shared understanding of cyber INT becomes a prerequisite when relevant stakeholders aim at establishing cooperation mechanisms in the field. This latter aspect is quite important. Indeed, the crafting process of cyber intelligence ideally requires mutual collaboration and knowledge sharing. To be effective and not fragmented, cooperation should be at least premised upon a common language and understanding of the conceptual components of cyber intelligence and its crafting process.

By defining cyber intelligence stricto or lato sensu (according to the already produced knowledge on the topic), identifying and structuring its conceptual components, as well as representing/interpreting them through a very basic (and preliminary) theoretical framework, the present paper contributes to explaining cyber INT. Needless to say that a more profound articulation of the framework is needed in order to grasp the different facets of cyber intelligence and better understand how this emerging practice could be established and further evolve.

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 to120 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