Campaign in Cyber or Cyber in the Campaign

Avner Simchoni

The field of cyber has acquired increasing legitimacy as an arena of action, as the international system becomes accustomed to its various uses for a range of needs. Israel sees cyber as a vital component of its national security, requiring investment and nurturing. From a historical point of view, the success of security and intelligence campaigns derives from smartly integrating new fields into the existing fabric—means, methods, and concepts—while implementing the necessary changes and adjustments. With the rapid introduction of cyber elements into our cognizance and systems, it is important to maintain perspective and to realize that while cyber is an important and expanding component, it is not a distinct, independent entity. This becomes even more valid when considering processes of situation assessment and decision making and the use of force in the face of threats on numerous fronts.

Keywords: Situation assessment, decision making, cyber, campaign, use of force, multi-disciplinary, technological revolutions

Background

We are currently at the height of a global trend in which the cyber dimension is becoming a central factor in all areas of life. This centrality creates dependence on cyber within developed countries and advanced economies as a vital pillar, beginning with conduct at the individual level, to economic

Avner Simchoni is a graduate of the Security Studies Program at Tel Aviv University and is a researcher in the fields of security and strategy. The author wishes to thank Brig. Gen. (Res.) Meir Finkel, commander of the Dado Center, for his helpful comments.

systems and how countries treat their citizens, and to its effect on global processes. At the same time, the involvement of cyber and its influence is evident in security and military aspects and increases as more systems are integrated into communications and computing.

Among the more prominent cyber events reported in 2016 were the following:

- attacks on essential infrastructures in Europe, including electricity systems
- attack on the Democratic Party servers in the United States
- attacks on targets in Vietnam
- the Locked Shields international cyber exercise with the participation of NATO states and other countries
- hacking of an electronic commerce system in India and the theft of details of some ten million customers
- the wide-ranging DDoS (distributed denial of service) attack on the American internet service provider DYN, and prolonged interference with activity on many important sites
- hacking and theft of tens of millions of dollars from the Central Bank of Bangladesh by means of the SWIFT mechanism (effective later action led to a considerable reduction of the amount stolen in this incident).[1]

The field of cyber is increasingly becoming a legitimate arena of action, as the international system becomes accustomed to the various uses of cyber for different needs. Governmental entities, or elements with government support, individual hackers, and "private" organizations are also active in the field—although with less intensity—and exploit the problem of attribution

[1] Meir Orbach, "Innovations of the Hackers Develop like Cyber," *Calcalist*, January 24, 2017 (in Hebrew); "President of Central Bank of Bangladesh Quits after 81 Million Dollars were Stolen from Bank Accounts by Hackers," *Globes*, March 15, 2016 (in Hebrew); Jim Finkle, "Bangladesh Bank Hackers Compromised SWIFT Software, Warning Issued," *Reuters*, April 25, 2016; Eric Lipton, David E. Sanger, and Scott Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," *New York Times*, December 13, 2016; Kyle York, "Dyn Statement on 10/21/2016 DDoS Attack," *Company News*, October 22, 2016, http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/; "Cyber-terrorists Attack Flight Info Screens at Vietnam's 2 Major Airports," *VnExpress,* July 29, 2016, http://e.vnexpress.net/news/news/cyber-terrorists-attack-flight-info-screens-at-vietnam-s-2-major-airports-3444504.html; "Locked Shields 2016," *NATO Cooperative Cyber Defense Center of Excellence*, April 18, 2016.

in cyberspace; we currently know of over half a billion malware programs active in cyberspace.

Unlike traditional fields of power, giant network and commercial corporations— mostly American, such as Google, Facebook, Microsoft, Twitter, Amazon, Apple—are also key players in this arena, closely pursued by Chinese companies (such as Huawei, Alibaba, and others). These giant corporations are far from being neutral platforms and have evolved into a kind of "gatekeeper" and new form of consciousness shaper: they are the ones that provide access and determine what the public will see and when, while countries and other international elements have almost no powers of regulation over them. To this, we can add cyber security and protection companies, which along with the internet corporations create a unique cyber environment. The big data revolution and high degree of connectivity resulting from the increasing implementation of IoT devices ("Internet of Things") have also increased awareness and exposure to cyber, as well as the assessment and investment by key players in cyber-related disciplines.

At the same time, diplomatic activity in the UN, NATO and other institutions (including at the bilateral level like the limited non-aggression pact between China and the United States in 2016) is working to formulate international norms and more effective, coordinated ways of handling shared cyber threats. Thus, authorities in the United States and other countries drew up demands for internal regulation of cyber challenges,[2] as well as for strengthening the ability of banks to deal with cyberattacks. At this stage, the focus of these demands is on providing backup and recovery capabilities for financial institutions in the face of serious cyberattacks; indeed, these institutions appear to be leading the private-civilian sector in investing in cyber defense.

According to a survey by the Fahn Kanne & Co. accounting firm, the annual financial damage due to cyber incidents worldwide is estimated at hundreds of billions of dollars.[3] It is also estimated that cyberattacks have reached second place in global financial crime, and they have affected about

[2] Tali Tsipori, "Regulation around the World: Government Dealings with the Cyber Challenges," *Globes*, April 5, 2016 (in Hebrew).

[3] Idan Rabi, "Annual Damage Worldwide caused by Cyberattacks—about 315 Billion Dollars," *Globes*, October 23, 2015 (in Hebrew).

35 percent of companies. Cases involving ransomware attacks rose by some 1000 percent last year, and these attacks are expected to increase.[4]

The targets of cyberattacks are varied: security elements, government and political bodies, the industrial and financial sectors (theft of business information and of money), databases, citizens, and even essential infrastructure.[5] Although it is difficult to quantify the damage caused by cyberattacks from the security-military aspect, it is clear that it is severe, and as a result, security establishments all over the world are investing huge resources to protect their systems. The former head of the CIA, David Petraeus, stated that "hackers are becoming more and more creative and wicked . . . Innovation in the field of hacking is developing like the cyber industry itself."[6]

This article seeks to clarify where Israel stands in relation to these trends, and specifically how Israeli activity in the cyber field should be integrated into the wider context of national security and address threats in the various arenas.

The Situation in Israel

Israel sees cyber as an essential component in its national security. As such, cyber requires continuous investment and nurturing so that Israel can maintain its leading position in the field of cyber on one hand and deal with the growing cyber threats from rivals and enemies on the other hand. This approach was already evident at the beginning of this decade with the National Cyber Venture Committee, led by Prof. Isaac Ben-Israel, who had been appointed by the prime minister. This committee outlined the principles for building an Israeli eco-system to facilitate optimal handling of the challenges of the cyber age. The vision and the goal that were defined in this framework were "to maintain Israel's status in the world as a development center for information technology and to ensure first class capabilities in cyberspace

[4] Aviv Levy, "Cyber Crime Has Climbed to Number 2 in the Economic Crimes in the World," *Globes*, November 8, 2016 (in Hebrew).

[5] Vindi Goel, "Yahoo Says 1 Billion User Accounts Were Hacked," *New York Times,* December 14, 2016.

[6] Orbach, "The Innovation of Hackers is developing like Cyber."

to safeguard its financial and national strength as an open, democratic and knowledge-based society."[7]

Like other countries and organizations, Israel is the target of cyberattacks on a daily basis. These attacks are designed not only to steal information and money but also to interfere with and damage production, management, and control systems. The number of attacks and attempted attacks amount to several thousand per day. A recent survey of 150 organizations in Israel found that a quarter of them had experienced a cyberattack during the previous three years by criminal elements, activists, and terror groups, affecting their routine conduct.[8] According to the Institute of National Security Studies, the cost of cybercrime in Israel is approaching ten billion dollars annually, including several billion dollars of damage from theft of commercial information.[9] Political, security, and other sensitive events are often the catalyst for increased attacks or for implementing latent capabilities in the cyber field.

Israel's lead in the field of cyber is manifested by policy and strategy outlines;[10] the activities of operative elements; the expansion of cooperation with international bodies; the technological development of security and

[7] Isaac Ben-Israel, "The National Cyber Project," *Ministry of Science and Technology*, May 2011. In this context, it is noted that as far back as 2002, Israel recognized in good time—partly thanks to the recommendation and involvement of the National Security Headquarters—the cyber threat to essential infrastructures and set up a special body to deal with these threats. See Yossi Melman, "The National Security Headquarters Will Benefit from the Elections," *Haaretz,* December 13, 2000 (in Hebrew).

[8] Ami Rojkes Dombe, "Half of the Respondents in the Survey 'State of Cyber Protection in Israel' are not Ready for a Cyberattack," *Israel Defense*, no. 29, May 2016 (in Hebrew).

[9] Rabi, "Annual Damage Worldwide Caused by Cyberattacks."

[10] See, for example, Rami Efrati and Lior Yaffe, "This is how to Build a National Cybernetic Defense," *Israel Defense,* August 11, 2012; "Policy of Regulation Cyber Defense Professions in Israel," *National Cyber HQ*, December 31, 2015. Activity in this field also takes place in the academic-research space. See, for example, Gabi Siboni and Ofer Assaf, *Guidelines for a National Cyber Strategy,* Memorandum 153 (Tel Aviv: Institute of National Security Studies, 2015); Ashton Carter, "Preface by Secretary of Defense," in Department of Defense, "The DoD Cyber Strategy," 2015.

civilian cyber products at the highest level;[11] the broad base of academic knowledge and infrastructure (currently five university research institutes work on the cyber field in Israel); and the training of skilled human capital in scientific disciplines connected to the cyber world and its implementation. There are about 400 cyber companies active in Israel,[12] and in 2015 they exported goods and services valued at billions of dollars, equal to about 10 percent of the total global cyber market. At the same time, Israel allocates—as well as attracts from outside—extensive funding for cyber R&D, which has been consistently rising over the last decade. Israel currently accounts for about 15 percent of total R&D investment worldwide in the field of cyber.[13] It should be noted that these figures change every year, as the global market grows, although Israel has maintained its leading place in both absolute and relative terms. The establishment of the Israeli cyber industry puts Israel in second place worldwide (in absolute terms) after the United States.[14]

The security system, the civilian sphere, and the private market in Israel maintain close mutual ties in the fields of training people and developing cyber skills: students acquire technological and scientific education before their military service; the technological system in the Israel Defense Forces (IDF) and the defense establishment trains and drills many people at the technological front; individuals leaving the defense system continue to advance cyber products and services in the private market and in security industries; and the academic world is working constantly to develop theoretical and practical knowledge. The state's investment, either directly or indirectly through its various arms, is discernible in most of the areas mentioned above.

In recent years, cybernetics has achieved a high status in the country, in accordance with the vision and purpose defined at the National Cybernetic Venture, the prime minister's policy, and decisions by the government and

[11] Prime Minister Benjamin Netanyahu, "Israel—World Cyber Power," *Globes*, April 3, 2016 (in Hebrew). It is also important to remember in this context the trend of advanced technologies and applications that germinate within military systems for meeting operational needs, and that are eventually further developed, and establish themselves in the civilian commercial market. Examples are computers and cellular devices.

[12] "The Israeli Cyber Security Map," *IVC Research Center*, January 2017.

[13] Meir Orbach, "15% of the World Investment in Cyber—in Israel," *Calcalist*, January 26, 2017 (in Hebrew).

[14] Amitai Ziv, "Cyber Power: The Sales of the Israeli Companies—10% of the World Transactions," *The Marker*, May 25, 2015 (in Hebrew).

the IDF. In January 2016, the prime minister stated in public that "cyber creates extensive financial opportunities. We want to be one of the five world cyber powers . . . to be a leader in this field. There are three main aspects of cyber: national, civilian and military . . . The first thing is that we have to immunize organizations and civilians. Every society and every person must be protected. The second thing is defense. [Thirdly,] there are large scale incidents that require a response against the attack and the attacker."[15] The prime minister spoke on this subject in public again, and stated that

> Cyber is linked to every industry today . . . The Internet of Things will create so [many] connections that we'll need a lot of solutions to cope with cyber defense . . . Cyber is also a new arena on the battlefield . . . With one press of a button, a lone hacker can bring a country to its knees. Nearly all the countries' infrastructures and intelligence are exposed to cyberattacks . . . A few years ago, I set an objective for Israel to become a leader in cyber. We have achieved that. We have also opened in research center in Beer Sheba. Israel accounts for about a fifth of global investment in the field of cyber. That's bigger than the population by a factor of 200 . . . We are developing Israel's human capital through training programs in the army and in academe.[16]

As for the growing cyber threat, the prime minister stated: "Terror organizations are using the same tools [that] we use— against us . . . In recent years Iran has been building a terror infrastructure in the Middle East. The Internet of Things can be used by these organizations for dangerous objectives. Unless we work together and cooperate, the future could be very threatening. In this context, Israel, the United States, and other countries must cooperate at government and industrial level."[17]

These understandings and decisions found expression in the allocation of resources; the establishment of new organizations and changes to existing ones; in the attention paid at command and administrative levels; the integration of cyber into theory; and programs for building up and operating forces. Among the steps taken in this context in recent years, we can mentioned the

[15] Raphael Kahan, "Netanyahu's Speech at Cybertech: 'We want to Lead the Field of Cyber Worldwide,'" *Calcalist*, January 26, 2016.

[16] Ami Rojkes Dombe, "Statement of the Prime Minister at the Cybertech Conference," *Israel Defense*, no. 31, January 2017.

[17] Ibid.

formation of the National Cyber Headquarters,[18] the National Authority for Cyber Defense,[19] the cyber setup in the various branches of the IDF,[20] the growing allocation of national resources, development of perceptions, drawing up regulations and implementing procedures,[21] expanding partnerships, and more. The field of cyber is also becoming more important in Israel's other security and intelligence entities and has become part of the mission of each organization.[22] A similar situation is taking place in other parts of the civilian system in Israel, including government ministries, statutory authorities, business entities, and public corporations.

Cyber as a Component of the Whole

The understanding that the future of cyber will be in "almost everything"—blurring traditional boundaries between civilian and defense, private and collective, national and international, the actual and the virtual—creates a challenge for state systems that seek to continue functioning at a high level and therefore require special preparations. In this context, we should mention the recent expansion of the national cyber network, whose purpose is to assist in realizing the national cyber vision and to create an environment that will support Israel's future prosperity and leadership in this field.

However, the profound effect of cyber is evident in other areas of security, intelligence, and the army, with emphasis on issues relating to the operating forces and managing military campaigns. A sufficiently broad historical perspective will show several other revolutions in technology, infrastructure,

[18] Promoting National Capability in Cybernetic Space, Government Resolution 3611, August 7, 2011.

[19] Promoting National Preparation for Cyber Protection, Government Resolution 2444, February 15, 2015.

[20] Gabi Siboni and Meir Elran, "Establishing an IDF Cyber Command," *INSS Insight*, no. 719 (July 8, 2015); Yossi Melman, "A Hole in the Network: Decision of the Commander in Chief not to Create an IDF Cyber Command is a Mistake," *Maariv*, 7 January 2017 (in Hebrew); Yossi Hatoni, Postponing the Establishment of a Cyber Command—A Justified Move," *People & Computers*, January 1, 2017 (in Hebrew).

[21] Promoting National Regulation and Government Lead in Cyber Protection, Government Resolution 2443, February 15, 2015.

[22] Itamar Eichner, "Exposure: Cyber Unit of the GSS from Within," *Ynet*, January 18, 2017 (in Hebrew); Eliran Rubin, "That's How You Missed the Chance to be Hackers in the Mossad," *The Marker*, May 15, 2016 (in Hebrew); Yossi Yehoshua and Reuven Weiss, "Geeks in the Dark," *Yedioth Ahronoth*, February 10, 2017 (in Hebrew).

and concepts that have had a profound and long-lasting influence on the battlefield and the world of intelligence and national security in general. These include weaponry, communications, traffic, data processing, means of collection, and more. The marked influence of cyber on concepts and practices that were commonly used until cyber appeared in its full intensity is essentially no different than the invention of explosives, the telegraph, the railway, the internal combustion engine, or flying.

Looking back, certainly to the start of the twentieth century, we can see that the success of armies and intelligence campaigns was usually the result of smartly integrating new means, methods, and concepts into the existing fabric, while making the necessary changes and adaptations. Examples are the use of railways to transport troops and equipment between fronts; the integration of tanks in battles and for moving over land; the harnessing of the computing revolution to gather information; or creating the capability for in-depth bombing using air forces. At the same time, some security failures were the result (even if not exclusively) of uncontrolled adoption or reliance on “the next new thing”—avant garde—such as the commanders behind the “plasma” screens. Here the intention is not to promote a reactionary or conservative approach that avoids all progress and unavoidable developments but rather to position change or revolution within the broader context.

At this point, I want to argue that it is within the context of the recent welcomed introduction of cyber into various systems (and the potential is still great) that as a historical lesson, we must maintain a broad perspective in all areas of security and intelligence and remember that cyber is just another tool—however large its scope and significance—to add to the constantly changing and existing arsenal. With all its importance and unique characteristics, above all, its immense influence in all areas of communication (interconnectivity), cyber should not be viewed as a distinctive, separate field when it comes to the processes of building and operating forces. Cyber is a multi-disciplinary field and not one-dimensional; it is not just “another technology” but rather a phenomenon with sociological, legal, economic, and other dimensions.[23] The multifaceted nature of cyber strengthens the need to integrate it into the fabric of the total system and not to isolate it.

[23] Yitzhak Ben Israel, “Cyber: Not What You Thought!” *CyberTech 2017*, January 2017, pp. 7–8.

The issue of deterrence in cyber also reflects the need for a holistic view. The problem of attribution makes it difficult to identify the object of deterrence and to adapt the tool for the required objective, although we can assume that the intensity of this problem will decline over time, as protective tools are improved.[24] The desirable answer to this question is that cyber deterrence does not have to remain within the field of cyber ("unique response") but can and should combine financial elements, international norms, and more. Prof. Nye argues that effective deterrence in cyber cannot be generic but rather needs to be adapted to each specific threat.[25] This understanding fits in well with the need to carry out a holistic assessment of a situation, allowing the use of a range of policy tools from different disciplines.

Some see cyber as a component of such enormous potential power (whether within or, as already mentioned, outside the field of cyber) that it can be used to project national strength to the outside world, analogous to a navy that controls the sea, the straits, marine commerce, marine battlegrounds, and more.[26] Perhaps this analogy is more suited to the first days of cyber, when advanced technology in this field seemed to be available only to superpowers; now it seems a little far-reaching, given the rapid proliferation of defensive cyber technology and other technologies. At the same time, this analogy does raise once again the enormous potential of cyber, which extends far beyond its narrow field, in a way that requires global and interdisciplinary observation.

As for the decision-making processes, the General Headquarters at the military level and the National Security Cabinet at the national level are the bodies in Israel responsible for overall observation—the holistic view—and for weighing all the inputs required for an integrative situation assessment as a basis for making decisions about building and using military force. Cyber is just one of the inputs, however great its importance. This is also how to interpret the statement by the prime minister about "large events that require a reaction against the attack and the attacker."[27] It is not correct to conduct an "assessment of the cyber situation" other than as a component of a general

[24] Joseph Nye, "Can Cyber Warfare Be Deterred?" *Project Syndicate*, December 10, 2015.

[25] Ibid.

[26] Joseph Nye, *Cyber Power* (Cambridge, MA: Belfer Center for Science and International Affairs, 2010), p. 4

[27] Kahan, "Netanyahu's Speech at Cybertech."

assessment, just as it is not correct to have a “National Security Council for Cyber” outside the integrated entity that is responsible for assessing the national situation—the National Security Council (NSC).[28] Just as nobody would think of having an “NSC for the Air Force” or a “General Headquarters (GHQ) for the Armored Corps,” in addition to the top-level leadership and command personnel, we must be careful of the tendency to manage a “national cyber campaign” as a separate system, rather than always seeing it as part of the wider system of the IDF or any other body, each according to its tasks and powers and all of them together as complementary parts of the entire national security.

It is correct and accepted to have headquarter entities for specific areas, both within the IDF and outside it, but these should be subordinate to the process of situation assessment and making decisions in the GHQ and the cabinet, with inputs from a range of sources, according to the rules of the GHQ as defined in GHQ Orders, in the NSC Law, and in other procedures. A situation in which a body that is responsible for a particular subject, no matter how important, also acts as the superintendent reflects an internal contradiction and raises the risk of interfering with the way top-level bodies should work and make decisions.

The National Information Directorate, established after the Second Lebanon War in 2006, based on the understanding of the importance of the public-media aspect of the campaign, is located in the Prime Minister’s Office, but it has no pretensions to replace any of the bodies actively engaged in providing information (the Foreign Ministry, the IDF spokesperson, and so on); the Counter Terrorism Bureau was established in the 1990s in the Prime Minister’s Office, and later made subordinate to the NSC, with the purpose of coordinating and improving cross-organizational cooperation in the field of fighting terror—in the face of the growing threat—but not to serve as a replacement for any of the security and intelligence entities. The products and bureaucratic location of these two bodies reflect the understanding that there is a need to strengthen the corporation between various government organsand that these matters need increased attention at the national level.

[28] See the National Security Headquarters Law, 5768–2008, which states that “The National Security Headquarters shall be the headquarters for the Prime Minister and the Government for all foreign and defense matters of the State of Israel” (Section 1b), and among other things shall prepare “an annual and long term assessment of the political-security situation” (Section 2a6).

However, they are not autonomous bodies nor "the last authority" in their fields but rather provide an important input to the integration and decision-making process at the political level, as a part of all the generic processes serving it.

Security entities must also be punctilious about introducing the "cyber input" to the mix of the overall situation assessment process, together with data and other inputs that may crop up, both "traditional" and new, for a complete process. If cyber is indeed "a new arena in the battle field,"[29] as the prime minister said, then the "cyber battle" must be conducted as another one of the battles that together form the campaign and not as a separate campaign. The former head of the CIA, David Petraeus, commented that "cyberattacks have already led to the imposition of sanctions, and it is obvious that we are entering a world where responses will depend on the severity of the damage. I believe that serious long-term damage to electricity systems will lead to a serious response. The response may involve cyber, diplomatic steps, sanctions or even a more serious response."[30] Cyber integrates with, affects, and is affected by other elements; in this situation of mutual links and influences, isolating cyber would be a methodological failure.

The placement of cyber in the correct context is also necessary from the organizational point of view. Since we are still in a relatively early stage of the cyber revolution and its integration into all spheres of life and into security systems, we cannot yet properly know the optimal way of organizing cyber in our systems in the future. Every organization naturally goes through changes over time, and organizational structures are shaped and abandoned based on accumulating experience. Indeed, in recent years various entities have been defining and updating their structure, while on the move, in a positive and necessary process of learning, adjustment, and adaptation. In view of both the objective and subjective difficulty of predicting how the relative position of cyber will be defined as part of the broad picture, it is essential to retain flexibility and a holistic view. Practical experience and learning processes, together with past examples and historical insights, will lead us, hopefully, to the optimal position. We can contribute to this, in terms of processes and organizations, if we ensure a proper balance and exposure

[29] Kahan, "Netanyahu's Speech at Cybertech."

[30] Orbach, "The Innovation of Hackers is Developing like Cyber."

to mutual influences between the various components, which in turn can also help to shape the field of cyber itself.

Conclusion

Cyber is continuing to stimulate profound changes in matters of security, the army, and intelligence. This is all part of its penetration into all systems of our lives and the huge social and economic revolution that accompanies it, which some are comparing to the agricultural, printing, and industrial revolutions, which changed the face of humanity. Cyber undermines traditional systems, and it integrates with contemporary trends that are challenging the existing liberal-democratic order that took root after the Second World War. Cyber is also changing the balance of power and the sources of authority that we have known until now, including concepts of sovereignty, territory, monopoly over the means of violence, and changing the ability to use force. As has already been shown, and according to widely accepted estimates, cyber embodies vast potential, for good and bad, and therefore requires enormous investment of resources and handling by all state entities, in both the national and international arenas. Consequently, the momentum and investment in all aspects of cyber development is inevitable, and it is all the more proper that Israel—through its security and civil organizations—leads the field in raising awareness of this.

At the same time, because of the rapid establishment of cyber in our various systems and as a result of our awareness, we must maintain a proper perspective, in which cyber is an important and growing element but not an independent or distinctive element. These words are even more apposite in relation to the issue of using force in the face of threats in different arenas. Taking a national view that is too narrow could lead to failures in assessing the situation, to organizational distortions, and ultimately even to errors when making decisions. A campaign will always be the result of inputs from a range of sources, creating a winning synergetic effect. Any bias towards a specific area, however important it may be, increases the risk of cognitive failures and mistaken decisions.

Just as a war is made up of a series of efforts and battles in various locations and of different types—sea, land, air, space, different geographical areas, political moves, financial aspects, technological and logistical considerations, and more—where it is the cumulative impact that leads to the final result, so too the world of cyber must be integrated into the total campaign in the political-security field. We must not try to conduct a separate "cyber campaign" that is independently managed but rather work for the smart integration of cyber into the general campaign, with all its considerations and aspects.

We have recently learned that an attack on the servers of the US Democratic Party during the 2016 presidential elections provoked a response (at least partially) in the diplomatic and public arenas. The conclusion is that the kinetic, the cybernetic, the media and the information effort, ground maneuvering, diplomacy, economic power and logistics—all these and others—create together the whole; accordingly, we must relate to all of its parts.