Cyber, Intelligence, and Security

Volume 2 | No. 2 | September 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. 2 | September 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)

The Cognitive Campaign: The Second Lebanon War as a Case Study

Pnina Shuker

The aim of this article is to examine the way that leaders try to shape their society's cognitive perceptions during war, with the assumption that society will not agree to unconditionally support a protracted war involving high casualties. Recognizing the necessity of large-scale public support of war, decision makers manipulate local public opinion so that it will justify the war and recognize the importance of the war's objectives and the ostensible achievements that war could provide. This article demonstrates how this was manifested during the Second Lebanon War—to the point of endangering the ground troops of the Israel Defense Forces for objectives that were purely psychological—and points out the negative repercussions of waging a war at the strategic level and on its outcomes.

Keywords: Cognitive battles, public opinion, domestic legitimization, national resilience, decision making

Introduction

In recent years, military strategy researchers have reached a consensus that civil populations increasingly influence the objectives of war, the choice of fighting modes, and sometimes even the management of the fighting itself.[1] A central component of this trend is the relationship of the public to war—

Pnina Shuker is a PhD candidate in the political science department at Bar-Ilan University and a research associate at the Institute of National Security Studies.

1 Stuart A. Cohen, "Changing Civil-Military Relations in Israel: Operational Repercussions," in *In the Name of Security*, ed. Majid Al-Haj and Uri Ben Eliezer (Haifa: Haifa University and Pardes Publishing, 2003), p. 103 [Hebrew].

which also has undergone drastic changes in contemporary times—and how cognitive tools and influence are used to shape public opinion.

Since the 1990s, protecting human life has become an extremely important operational consideration,[2] and during the 2000s, society had developed an expectation of war without casualties.[3] The assumption underlying this article is that this expectation—as perceived by decision makers—considerably influenced the combat doctrine of the Israel Defense Forces (IDF) during the Second Lebanon War, leading at the same time to an incessant cognitive campaign vis-à-vis target audiences in Israel in order to retain public support for the war. This article engages, therefore, in the importance attributed to inculcating a sense of victory among the Israeli public during that war.

The article begins with a theoretical review of the phenomenon of the sensitivity of democratic society to casualties and, as an outcome, the importance of the military campaign to gain the home society's cognitive support. The article then looks at the entrenching of the cognitive aspect in the IDF, while examining the question of how this was manifested during the Second Lebanon War. Finally, the article will elaborate on the possible negative repercussions as a result of attributing excessive importance to the cognitive dimension.

The Importance of the Cognitive Campaign

Researchers have not agreed upon any uniform definition of the essence of the war over cognitive perceptions. Col. (res.) Miri Eisin, the former international media spokesperson of the Israeli government, proposed the following definition: "The battle over cognitive perceptions during a war is the overall attempt of a country or a non-state entity to influence various target audiences in order to achieve a victory in a national struggle."[4] According to Saar Raveh, the term "cognitive arena" is relatively new in the field of the military and warfare and relates to a number of central processes that emerged

2 Yagil Levy, "The Social Dimension of Civilian Control over the Military: Policy of Preventing Casualties," in *Military-Civilian Relations in Israel: Implications on War and Peace Decision-making,* ed. Ephraim Lavi (Tel Aviv: Tami Steinmetz Center for Peace Research, Tel-Aviv University, 2013), p. 71 [Hebrew].

3 Meir Finkel, "Society's Impact on IDF Doctrine and Culture," *Ma'arachot* 412 (May 2007): 61 [Hebrew].

4 Reuven Erlich, "The Contribution of Intelligence in the War over Perceptions," *Meir Amit Intelligence and Terror Information Center*, July 11, 2006.

since the end of World War II and continue to this day. These processes include the changing nature of the confrontations in which militaries in general and the IDF in particular are involved; the intensifying involvement of the world powers in ethnic or national disputes beyond their borders; and, concurrently, the rise in the importance of global public opinion; and transformations in the realm of information, which has led to the creation, ownership, and dissemination of information that is not under the control of any authority. These processes have transformed the military's physical operations into campaigns integrated with operations in the cognitive realm, which seek to explain, interpret, and define to target groups the objectives of the military operation, its targets, and even its outcomes, in a way that reflects the policy and the interests of the initiator of the operation.[5]

According to Lior Reshef and Shay Shabtai, another dimension of the military campaign is cognitive, which relates to subjective aspects such as thoughts, beliefs, perceptions, world views, interpretations, and symbols. The cognitive dimension involves an incessant process of imparting meanings to events that take place in reality, and consequently, is vulnerable to manipulation and influence. It is saturated with variables and players, and in order to create an effective influence, congruence is needed between the various efforts that shape the reality—particularly, the force deployment—and the "story" that the IDF wants to convey to the target audiences.[6]

In the years preceding the Second Lebanon War, the IDF began to understand that dealing a serious blow to the enemy's ability to fight relates to the cognitive aspect of the military operation no less than the physical aspect.[7] Under Chief of Staff Moshe Ya'alon, the IDF understood the importance and necessity of shaping the cognitive perceptions of Israeli society as well as that of the enemy. Within this framework, the Center for Cognitive Operations was established in January 2005, with the mission of examining the cognitive aspects of the military operations and initiating operations geared toward influencing the enemy's perception, mainly through propaganda, psychological warfare, and sometimes deceptive tactics. The Center for Cognitive Operations was directly subordinate to the head of the

5 Saar Raveh, "Cognition and Experience: The Two Components of the Operational Whole," *Ma'arachot*, 409–410 (December 2006): 66–68 [Hebrew].

6 Lior Reshef and Shay Shabtai, "The Cognitive Effort in the IDF," *Ma'arachot*, 457 (October 2014): 35 [Hebrew].

7 Raveh, "Cognition and Experience," p. 71.

IDF Operations Directorate, which attests to its considerable importance.[8] Another unit with a similar mission had existed previously, but its operations were quite limited.[9]

Chief of Staff Dan Halutz adopted a similar approach, whereby every war is, first and foremost, a battle over cognitive perceptions.[10] He believed in the need to influence the enemy's cognition and formed a "Campaign Design Department" for this purpose in the Operations Directorate.[11] The IDF Spokesperson's Unit also adapted its aims to the systemic approach: no more engaging in spokesmanship and propaganda but rather in the "design of a perception of reality in the public discourse." It was determined that the IDF needed to deploy a "cognition system" in times of war, exactly like the conventional systems in command centers that are responsible for launching fire power or for coordinating logistical assistance. A "cognition system" was established even in the IDF's Galilee Division, which is responsible for the Lebanese front; in other words, at issue was a combat system for all intents and purposes.

Democratic Society's Sensitivity to Casualties

The phenomenon of sensitivity to casualties is defined as a society's aversion to suffering losses during a military operation. There is wide consensus that this phenomenon has been a constant social and cultural characteristic of western democracies since the end of the Cold War, and that it is increasing to the point of absolute opposition to launching operations that could involve

8 Yoni Shedmi and Barak Ravid, "The Unit that will Drive Our Enemies Crazy," *Maariv NRG*, December 17, 2005 [Hebrew].

9 Ron Schleifer, "Psyoping Hezbollah: The Israeli Psychological Warfare Campaign during the 2006 Lebanon War," *Terrorism and Political Violence* 21, no. 2 (2009): 223.

10 Matt M. Matthews, "Hard Lessons Learned: A Comparison of the 2006 Hezbollah-Israeli War and Operation Cast Lead: A Historical Overview," in *Back to Basics: A Study of the Second Lebanon War and Operation Cast Lead*, ed. Scott C. Farquhar (Fort Leavenworth, KS: Combat Studies Institute Press, US Army Combined Arms Center, 2009), p. 44.

11 Amir Rapaport, *Friendly Fire: How We Failed Ourselves during the Second Lebanon War* (Tel Aviv: Sifriat Maariv, 2007), pp. 53–54 [Hebrew]; Schleifer, "Psyoping Hezbollah," p. 224.

casualties.[12] Some argue that the phenomenon restricts the militaries, in that it might motivate leaders to adopt a policy of casualty aversion; that is, a policy that strives to limit the risks to the combat forces, and it sometimes might escalate to the point of sacrificing operational efficiency and even refraining from missions in which casualties are expected.[13]

Some researchers believe that society's sensitivity to casualties will diminish as long as it believes that the prospects of victory during the war are high. In other words, even if the public perceives that launching the war is a mistake, it will accept the continuation of the fighting and will reconcile itself to additional casualties if it sees that its side is winning.[14] Thus, during wartime, leaders consider it highly important to give the public a sense that

12 Gerhard Kummel and Nina Leonhard, "Casualties and Civil-Military Relations: The German Polity Between Learning and Indifference," *Armed Forces & Society* 31, no. 4 (2005): 514–515; Joseph Soeters and Jan Van Der Meulen, "Considering Casualties: Risk and Loss during Peacemaking and Warmaking," *Armed Forces & Society* 31, no. 4 (2005): 483; Joseph P. Vasquez, "Shouldering the Soldiering: Democracy, Conscription and Military Casualties," *Journal of Conflict Resolution* 49, no. 6 (2005): 849; Yagil Levy, *Israel's Death Hierarchy: Casualty Aversion in a Militarized Democracy* (New York: New York University Press, 2012), p. 2.

13 Edward N. Luttwak, "Where Are the Great Powers? At Home with the Kids," *Foreign Affairs* 73, no. 4 (1994): 24; Edward N. Luttwak, "A Post-Heroic Military Policy," *Foreign Affairs* 75, no. 4 (1996): 42; Harvey Sapolsky and Jeremy Shapiro, "Casualties, Technology, and America's Future Wars," *Parameters* 26, no. 2 (1996): 122; James Burk, "Public Support for Peacekeeping in Lebanon and Somalia: Assessing the Casualties Hypothesis," *Political Science Quarterly* 114, no. 1 (1999): 54; Philip Everts, "When the Going Gets Rough: Does the Public Support the Use of Military Force?," *World Affairs* 162, no. 3 (2000): 93.

14 Jeffrey Record, *Hollow Victory: A Contrary View of the Gulf War* (Washington: Brassey's, 1993), p. 137; Steven Kull, "Review of Eric Larson's Casualties and Consensus," *Public Opinion Quarterly* 61, no, 4 (1997): 672; Marijke De Konink and Jan Van Der Meulen, "Risky Missions: Dutch Public Opinion on Peacekeeping in the Balkans," in *Public Opinion and the International Use of Force*, ed. Phillip Everts and Pierangelo Isernia (London: Routledge, 2001) p. 116; Peter D. Feaver, Christopher Gelpi, and Jason Reifler, "Success Matters: Casualty Sensitivity and the War in Iraq," *International Security* 30, no. 3 (2005): 7–8; John E. Mueller, "The Iraq Syndrome," *Foreign Affairs* 84, no. 6 (2005): 49; Patricia L. Sullivan, "Sustaining the Fight: A Cross-Sectional Time-Series Analysis of Public Support for Ongoing Military Interventions," *Conflict Management and Peace Science* 25, no. 2 (2008): 112; Peter D. Feaver, Christopher Gelpi, and Jason Reifler, *Paying the Human Cost of War: American Public Opinion and Casualties in Military Conflicts* (Princeton: Princeton University Press, 2009), p. 1.

victory is imminent, inter alia, by presenting achievements on the battlefield, as well as by obfuscating facts that might cause demoralization, such as mistakes, defeats in battle, and heavy losses.[15]

According to Cornish, another way to prevent demoralization is to falsely report the number of fatalities. However, reporting a number of fatalities that is lower than the real number may raise the public's threshold for similar outcomes in future military operations. Thus, instead of reducing society's sensitivity to casualties, the opposite outcome is achieved.[16] The research literature describes additional ways to "soften" the information about the number of fatalities, such as eliminating particular types of casualties from the inclusive total; controlling the photos published of fallen soldiers in order to avoid exacerbating the public outrage; releasing details about fatalities simultaneously with news about achievements during the war in order to create a sense among the public that the sacrifice was worthwhile.[17] This article argues that tremendous efforts were exerted during the Second Lebanon War to internally legitimize the fighting and to create a sense of achievement compared to the number of casualties.

Sensitivity to Casualties during the Second Lebanon War

Many researchers have argued that the political and military echelon hesitated in carrying out extensive ground operations during the Second Lebanon War, which could have reduced the number of rockets fired on Israel's citizens,

15 Tirza Hechter, "Political Myths—Continuity versus Change: The Development of Political Myths Surrounding the Yom Kippur War Among the Secular Jewish Public: from the Yom Kippur War until the Oslo Agreement," (PhD diss., Bar-Ilan University, 1996), p. 55 [Hebrew].

16 Paul Cornish, "Myth and Reality: US and UK Approaches to Casualty Aversion and Force Protection," *Defense Studies* 3, no. 2 (2003): 124.

17 Douglas L. Kriner and Francis X. Shen, *The Casualty Gap: The Causes and Consequences of American Wartime Inequalities* (New York: Oxford University Press, 2010), p. 9.

because they were overly sensitive to the soldiers' lives.[18] According to Yagil Levy, in July 2006, the decision makers were given little legitimacy to send ground forces in to Lebanon as it would also require the call-up of reservists.[19] Dan Halutz, then the chief of staff, also asserted that Israel was facing a campaign based on deploying long trajectory fire, mainly by means of the air force and artillery.[20] He also expressly decided to avoid a ground

18 Yitzhak Ben-Israel, *The First Missile War: Israel-Hezbollah* (Tel Aviv: Tel Aviv University, Harold Hartog School of Government and Policy, 2007), p. 20 [Hebrew]; Yehuda Wegman, "A Distorted Self-Image: On the IDF and its Responsibility for Civilians," *Strategic Assessment* 10, no. 2 (2007): 24 [Hebrew]; Efraim Inbar, "Strategic Follies: Israel's Mistakes in the Second Lebanon War," in *The Second Lebanon War and Subsequently* (Ramat Gan: Bar-Ilan University, Begin-Sadat Center for Strategic Studies, 2007), pp. 4–5 [Hebrew]; Dov Tamari, "Can the IDF Change After the Second Lebanon War?," *Ma'arachot*, 415 (2007): 38 [Hebrew]; Ron Tira, *The Battle over the Nature of War: From Clausewitz to Scipio Africanus and from Anwar Sadat to the Political Enemy who became Accustomed to War against the RMA* (Tel-Aviv: Institute of National Security Studies, 2008), p. 97 [Hebrew]; Moshe Ya'alon, "The Link between the Political Echelon and the Military Echelon when Preparing Ground Maneuvers," lecture at the Second Latrun Military Defense Conference, Latrun, Armored Corps Memorial, September 16, 2008 [Hebrew]; Giora Segal, "The Criticality of Ground Maneuvers during an Asymmetric Confrontation," *Strategic Assessment* 10, no. 4 (2008): 24, 28–30 [Hebrew]; Amir Harpaz, "New Roles of Ground Maneuvers," *Ma'arachot* 431 (2010): 21 [Hebrew]; Uzi Rubin, *The Rocket Campaign against Israel during the 2006 Lebanon War* (Ramat-Gan: Bar-Ilan University, The Begin-Sadat Center for Strategic Studies, 2008), p. 16; Avi Kober, "The Israel Defense Forces in the Second Lebanon War: Why the Poor Performance?," *Journal of Strategic Studies* 31, no. 1 (2008): 7; Uri Bar-Joseph, "The Hubris of Initial Victory—the IDF and the Second Lebanon War," in *Israel and Hizbollah: An Asymmetric Conflict in Historical and Comparative Perspective*, ed. Clive Jones and Sergio Catignani (London: Routledge, 2009), p. 153.

19 Yagil Levy, "How Democratization Spawns Militancy—the Second Lebanon War," *Politica* 17 (2008): 122 [Hebrew].

20 Giora Segal, "How to Beat Revolutionary Forces," *Ma'arachot* 415 (2007): 44 [Hebrew]; Uri Ben-Eliezer, *Israel's New Wars: A Sociological-Historic Explanation* (Tel-Aviv: Tel Aviv University, 2012), pp. 393–394 [Hebrew]; Haim Rosenberg, "Technology will Not Replace Maneuvers," *Ma'arachot* 443 (2012): 74 [Hebrew]; Stuart Cohen, *Israel and its Army: From Cohesion to Confusion* (London: Routledge, 2008), p. 46; Efraim Inbar, *Israel's National Security: Issues and Challenges since the Yom Kippur War* (London: Routledge, 2008), p. 226.

operation and disregarded the "Mei Marom" contingency plan designed for the circumstances that Israel had encountered on the morning of July 12, 2006.[21]

After the war, Halutz claimed that when he made decisions during the war, it had been clear to him that he needed to consider the parents of 2006, as the tolerance for casualties had changed from what it had been in the past.[22] And indeed, upon the launch of the campaign, Halutz submitted a recommendation to the government to attack the national infrastructure in Lebanon; however, the prime minister opposed a large-scale assault due to the American opposition.[23] Nonetheless, the government did approve an attack on the airport runways in Beirut and on the Beirut-Damascus highway. [24]

The Winograd Committee, which investigated the Second Lebanon War, found that the military activity had continued until the end of the war under routine security procedures and prohibitions and had imposed restrictions on the forces' actions, compatible with routine security considerations, such as avoiding the endangerment of soldiers.[25] Halutz also referenced this in his book, writing that "the failure to internalize the situation of the war found expression in the various internal directives issued by the Northern Command, by the Navy and by the Air Force, and they imposed constraints

21 Giora Segal, "The Second Lebanon War—the Missed Opportunity," *Ma'arachot* 420–421 (2006): 17 [Hebrew]; Michael Harsgor and Ehud Fuchs, *Historical Decisions and Hysterical Decisions* (Or Yehuda: Dvir, 2010), p. 326 [Hebrew]; Matt M. Matthews, *We Were Caught Unprepared: The 2006 Hezbollah-Israeli War* (Fort Leavenworth, KS: US Army Combined Arms Center, Combat Studies Institute Press, 2008), p. 43; Benjamin S. Lambeth, *Air Operations in Israel's War Against Hezbollah: Learning from Lebanon and Getting it Right in Gaza* (Santa Monica: Rand, 2010), p. xv.

22 Gal Hirsch, *Love Story, War Story* (Tel Aviv: Hemed Books, 2009), p. 330 [Hebrew].

23 Anat Tal-Shir and Zadok Yehezkeli, "Government in Darkness," *Yedioth Ahronoth* August 18, 2006, pp. 8–9 [Hebrew]; Rapaport, *Friendly Fire*, p. 22; Amos Harel and Avi Issacharoff, *Spiderweb: The Story of the Second Lebanon War* (Tel-Aviv: Yedioth Ahronoth, 2008), p. 165 [Hebrew]; Eyal Zisser*, Lebanon Blood in the Cedars* (Tel Aviv: Hakibbutz Hameuchad, 2009), p. 206 [Hebrew]; Zaki Shalom, "Defining the Enemy in an Asymmetrical Confrontation: The Case of the Second Lebanon War," *Strategic Assessment* 12, no. 3 (2009): 8–10 [Hebrew]; Amir Eshel, "En Route to a Standstill in Maneuvers," *Ma'arachot* 434 (2010): 24 [Hebrew]; Bar-Joseph, "The Hubris of Initial Victory"; Kober, "The Israel Defense Forces in the Second Lebanon War," p. 36.

24 Rapaport, *Friendly Fire*, p. 173.

25 Winograd Committee, *Second Lebanon War: Final Report* (Jerusalem, 2008), p. 314 [Hebrew].

and restrictions on the operational forces that were incompatible with the reality of the war they had entered. The fear of soldier casualties had become deep-seated."[26]

Perception of Victory during the Second Lebanon War

Many attempts were made during the Second Lebanon War to generate a "image of victory."[27] Chief of Staff Halutz declared that "the strategy is to create the perception of the weakening of Hezbollah, inter alia, by capturing/killing the organization's terrorists and giving public resonance to the matter."[28] Therefore, throughout the fighting, IDF forces were ordered to document and photograph evidence in the field, including bodies of Hezbollah terrorists, in order to illustrate their victories.[29]

According to a senior IDF officer, "They constantly wanted us to bring photos of dead terrorists, of terrorists who are raising their hands, in order to shape public perception.[30] To this end, a procedure was issued called "operational documentation," and some of the combatants were equipped by the IDF spokesperson with about two hundred various still and video cameras, some of which were attached to their helmets.[31] One of the assignments of a brigadier-general at the IDF Headquarters in Tel-Aviv was to receive the operational documentation.[32] Just how important this documentation was can

26 Dan Halutz, *At Eye Level,* (Tel Aviv: Yedioth Ahronoth, Hemed Books, 2010), p. 386 [Hebrew].

27 Harel and Issacharoff, *Spiderweb,* p. 398.

28 Harel and Issacharoff, *Spiderweb,* p. 236.

29 Felix Frisch, "IDF Soldier Protest and Photos of Terrorists' Bodies," *Maariv*, July 6, 2007, p. 11 [Hebrew].

30 Eitan Glickman and Nava Tzuriel, "The Vale of Tears," *Yedioth Ahronoth,* August 16, 2006, p. 9 [Hebrew].

31 Amir Rapaport, "The IDF Broadcast Photographs of Hezbollah Fatalities on Al-Manar," *Maariv*, August 9, 2006, p. 19 [Hebrew]; Yael Sloma and Lilach Shuval, "In the Propaganda Arena: Combatants are Equipped with Cameras to Document the Activity," *BaMahane*, July 27, 2006, p. 7 [Hebrew]; Nurit Kenti, "Our Functioning was Excellent," *HaAyin HaShevi'it* 64 (2006), p. 13 [Hebrew]; The State Comptroller Office, "Aspects in the Organization and Functioning of the Propaganda Personnel during the Second Lebanon War," in *Annual Audit Report 58.A for 2007* (Jerusalem: State Comptroller's Office, 2007), p. 483 [Hebrew]; Shulamit Shavit, "Photographs of the Victory," *Ma'arachot* 440 (December 2011): 59 [Hebrew].

32 Yoav Limor and Ofer Shelah, *Captives in Lebanon: the Truth about the Second Lebanon War* (Tel Aviv: Yedioth Ahronoth, 2007), p. 270 [Hebrew].

be understood from the chief of staff's summary of August 8, 2006, which stated that "This is a supportive, helpful, and meaningful component to the success of the operations. We must be diligent about this documentation at all levels, and about the rapid dissemination of its products.[33] In fact, the operational documentation effort produced little output, and in the final analysis, most of the visual material presented during the war came from photographs by the air force.[34]

The Command and Chief of Staff Halutz both pressured the forces to capture Hezbollah combatants.[35] "Bring me bodies and captives," Halutz repeatedly said to Northern Command personnel, saying "I want ten captives in every mission."[36] One of the commanders at the front also attested, "They told us: bring as many bodies of Hezbollah combatants and captives in their underwear as you can."[37] Maj. Gen. Eyal Ben-Reuven, who served as an advisor to Head of Northern Command Maj. Gen. Udi Adam during the fighting, expressed harsh criticism after the war, stating that "It also disturbed me that the Northern Command was required, time after time, to bring corpses of terrorists and photographs of terrorists. This demand from commanders and soldiers is unreasonable . . . you gain a cognitive achievement by defeating the enemy and not by lugging corpses of terrorists on stretchers.[38]

During the war, several controversial military operations were carried out that were harshly criticized for jeopardizing soldiers for the sake of obtaining the desired "victory picture." I chose to focus on three key examples: the battles in Bint Jbeil, Operation "Sharp and Smooth," and the launch of the ground operation toward the end of the war.

---

33 State Comptroller's Office, "Aspects in the Organization and Functioning," p. 468.

34 State Comptroller's Office, "Aspects in the Organization and Functioning," p. 483, Knesset Subcommittee on Foreign Relations and Public Relations, "Report on Israel's Public Relations System during the Second Lebanon War," December 2007, p. 17 [Hebrew]].

35 Ilan Kfir, *The Ground Trembled* (Tel Aviv: Sifriat Maariv, 2006), p. 185 [Hebrew].

36 Limor and Shelah, *Captives in Lebanon*, p. 160; Rapaport, *Friendly Fire,* p. 174; Harel and Issacharoff, *Spiderweb*, pp. 244, 398; Amir Rapaport, "The Night When the Knives were Drawn," *Maariv*, June 29, 2007, p. 12 [Hebrew].

37 Ronen Bergman, "Collapse of Concept 2," *Yedioth Ahronoth*, August 18, 2006, p. 36 [Hebrew].

38 Amira Lam, "The Contingency Plan Failure," *Yedioth Ahronoth*, March 9, 2007, p. 34 [Hebrew].

The Battles in Bint Jbeil

The majority of the Israeli campaign during the Second Lebanon War was conducted from the air; nevertheless, at a particular stage, the IDF ground forces were ordered to take over the town of Bint Jbeil, which had not been a target of any considerable strategic importance,[39] except that it was considered "the capital of the Hezbollah," where Hassan Nasrallah, the organization's secretary-general, delivered his infamous speech after the Israeli withdrawal from Lebanon in 2000, during which he referred to Israel as weaker than a spiderweb.[40] According to Harel and Issacharoff, the intention had been to bring the prime minister and the minister of defense to the place where Nasrallah had made his speech so that they could deliver their own victory speech; however, by the end of the war, this was no longer possible.[41] Maj. Gen. Benny Gantz, commander of the ground forces, had conceived the idea for the operation in Bint Jbeil believing that it would be a significant achievement in one place: "Nasrallah's victory speech was in Bint Jbeil . . . I would consider a limited ground mission in this region, which can be contained . . . I would bring in a film team to show the course of action and its results. In other words, it tells the complete story."[42]

Chief of Staff Halutz supported Maj. Gen. Gantz's idea,[43] and said that "modern wars are wars over symbols. Bint Jbeil is a symbol. Nasrallah gave his spider web speech in Bint Jbeil. There are symbols here that they defended, and our role now is to show them that we are striking them in this place."[44] Maj. Gen. Gadi Eizenkot, who had served as the head of the

39 Bar-Joseph, "The Hubris of Initial Victory," p. 154.

40 Moshe Ya'alon, *Long Short Road,* (Tel Aviv: Yedioth Ahronoth, Hemed Books, 2008), p. 208 [Hebrew]; Ze'ev Schiff, "The Head of the Military Intelligence Directorate had Warned the Prime Minister in Advance: Expanding the Operation is a Mistake," *Haaretz*, September 7, 2006 [Hebrew]; Oded Lowenheim, "Legitimizing Victims during War," (lecture Open University, November 13, 2011); Amir Rapaport, "The IDF and the Lebanon Syndrome—Toward the Third Lebanon War?," (paper presented at conference the Lebanese Arena—Marking Thirty Years since the Lebanese War, Bar-Ilan University, Begin-Sadat Center for Strategic Studies, May 30, 2012).

41 Harel and Issacharoff, *Spiderweb*, p. 260.

42 Amir Rapaport, "Go In, Kill some Terrorists, Get Out," *Maariv,* July 6, 2007, pp. 18–19 [Hebrew].

43 Gadi Heimann and Oded Lowenheim, "'Proper Retribution': Revenge and the Israeli Campaign during the Second Lebanon War," *Politica* 17 (2008): 103 [Hebrew].

44 Rapaport, *Friendly Fire*, pp. 160–161.

Operations Directorate at that time, also argued during the war that "what is important is the symbol, the ability to do this, and to shatter the myth."[45] The name that was given to the operation in Bint Jbeil—"Web of Steel" in response to Nasrallah's spiderweb theory—attests to the considerable cognitive importance that was attributed to it.[46]

The operation, which was launched on July 24, was indeed perceived as a success by the Northern Command; the General Staff, however, had expected achievements with far greater symbolic value, such as taking captives. Thus, even though on the evening of July 24, the forces had been ordered to retreat toward Israel, at the last moment, the Golani Brigade was ordered to remain in the field for the purpose of seizing the town.[47] Maj. Gen. Adam, who doubted the wisdom of the order, decided on his own to not seize the town—out of concern for the high price of casualties— and instead, deepened the hold over it. Nonetheless, two days later, on July 26, a bloody battle took place in Bint Jbeil, in which eight combatants were killed.[48]

Given the outcome of the Battle of Bint Jbeil, the desire for a cognitive achievement increased. Minister of Defense Amir Peretz remarked after learning about the number of fatalities that "we need to take a deep breath, and change the picture. If it had been possible to consider ending the war with partial achievements, it is now more distant . . . we cannot leave now with our tails between our legs, without dignity."[49] After the battle, Maj. Gen. Eyal Ben-Reuven expressed harsh criticism to Chief of Staff Dan Halutz about the futility of the mission, stating that "Occupying Bint Jbeil is contrary to the combat mission of reaching areas where Katyusha rockets are being launched . . . out of the five brigades that we have, we destroyed three over nothing, even before the ground war against the Katyusha rockets began."[50]

On July 27, Deputy Chief of Staff Maj. Gen. Moshe Kaplinsky claimed that "there is no tactical military significance to seizing Bint Jbeil. It has

45 Rapaport, "Go In, Kill some Terrorists, Get Out," p. 20.

46 Heimann and Lowenheim, "'Proper Retribution,'" p. 103; Harel and Issacharoff, *Spiderweb*, p. 252.

47 Amir Rapaport, "We Engaged, There are Injuries," *Maariv*, July 13, 2007, pp. 16–19 [Hebrew].

48 Nahum Barnea and Shimon Schiffer, "The Longest Day," *Yedioth Ahronoth,* July 28, 2006, p. 4 [Hebrew].

49 Rapaport, "We Engaged, There are Injuries," p. 18.

50 Ibid.

another significance . . . the symbolic significance."[51] Chief of Staff Halutz accepted Kaplinsky's position, and on July 28, the order was issued once again to capture the town, but was rescinded the next day after another attempt by the 101st Paratrooper Brigade to seize Bint Jbeil.[52] On August 1, the forces of the Ninety-First Division were ordered to launch an additional attack on Bint Jbeil,[53] and even when the IDF already began planning the major ground operation that was intended to push back the Katyusha rockets, the chief of staff did not waive capturing the town.[54] On August 7, the paratrooper's brigade were ordered to enter Bint Jbeil once again, to reach the building that had been used as the headquarters of the Western Brigade in the buffer zone prior to the May 2000 withdrawal, to raise the Israeli flag there, and to photograph it. Ironically, this operation later was given the nickname "the flag attack."[55] In addition, a victory march was planned: A convoy of tanks and armored personnel carriers was supposed to travel along Bint Jbeil's main street, and an appropriate victory speech, which was intended to refute Nasrallah's claims regarding the weakness of Israeli society, was written ahead of time for the commander of the occupying force, Brigade Commander Hagai Mordechai. Combatants equipped with video and still cameras were asked to document the historic speech and the Israeli flag on the building of the former brigade headquarters.

Brigade Commander Mordechai had reservations about the idea, and he had good reason for this: When he received the order, he and his forces were already a few kilometers north of Bint Jbeil, en route to seize control over the areas from where Hezbollah was launching Katyusha rockets aimed at Israel.[56] At this stage of the fighting, the commander of the Ninety-First Division, Brig. Gen. Gal Hirsch, also did not support seizing the town. "We are already located in the front," he argued to Maj. Gen. Ben-Reuven. But

51 Limor and Shelah, *Captives in Lebanon*, p. 266.

52 Ibid., pp. 191–192.

53 Winograd Committee, *Second Lebanon War*, p. 368.

54 Rapaport, *Friendly Fire*, p. 259.

55 Amos Harel, "The Version of Brig. Gen. Hirsch: the Criticism of the Propaganda about the Ninety-First Division's Achievements," *Haaretz*, September 11, 2006 [Hebrew].

56 Rapaport, *Friendly Fire*, pp. 259–260.

the latter explained to the division commander that they had no choice: The chief of staff wanted a cognitive achievement.[57]

At the beginning of the battle, it seemed that the Hezbollah force in Bint Jbeil was about to collapse, but then, one of the soldiers in the paratrooper commando unit was mortally wounded. A battle began in order to rescue him, during which another soldier was killed.[58] The mission was not abandoned, however, and it was decided to call in the 890th Paratrooper Division. In the end, the Israeli flag was photographed flying over a building adjacent to the building where the hoisting of the flag was originally intended.[59] The photographs were forwarded to the IDF Spokesperson's Unit but were archived. The outcomes of this battle only deepened the call to launch an even more drastic action that would change the cognitive picture.[60]

Operation Sharp and Smooth

During the war, special operations were carried out deep in enemy territory unlike the IDF had known before.[61] The decision makers believed that a surprise commando operation in the enemy's home front would enable them to achieve cognitive achievements that would strengthen the public's confidence in the war's leadership.[62] Consequently, besides the effort to strike the Hezbollah leadership, Prime Minister Olmert and Minister of Defense Peretz pressured Chief of Staff Halutz to carry out special operations similar in style to Operation Entebbe.[63] "I need something like the IDF of the olden days," said the prime minister.[64] Instead of directly contending with the threat of the Katyusha rockets, the desire was to carry out an operation that

57 Hirsch, *Love Story, War Story*, p. 352.

58 Kfir, *The Ground Trembled*, p. 207.

59 Harel and Issacharoff, *Spiderweb*, p. 349.

60 Limor and Shelah, *Captives in Lebanon*, p. 208.

61 Alex Fishman, "Mission Impossible," *Yedioth Ahronoth,* October 27, 2006, p. 10 [Hebrew]; Halutz, *At Eye Level*, p. 467; Ronen Cohen, "The Difference between a Strategic Incursion and a Tactical Incursion," *Israel Defense*, February 27, 2012 [Hebrew].

62 Kfir, *The Ground Trembled*, p. 191; Limor and Shelah, *Captives in Lebanon*, p. 260.

63 Moran Weinreich, "A New Generation of Warfare—Really? The Second Lebanon War," (MA diss., Bar-Ilan University, 2010), p. 90 [Hebrew].

64 Bergman, "Collapse of Concept 2," p. 34.

would shatter the symbol of the Hezbollah and provide an image of victory that would influence the public's cognitive perception.[65]

On the ninth day of the war, a special team was assembled in the Operations Directorate, headed by Brig. Gen. Tal Russo,[66] and the special units—the General Staff Reconnaissance Unit, the Kingfisher Unit, the Commando Unit, and others—began operational planning, as well as a search for a target that would provide the necessary cognitive effect.[67] Concurrently, special teams inside the divisions were deployed along the front line.[68] In total, twenty-four special operations were carried out during the war north of the Litani River, most of which were covert operations.

Operation "Sharp and Smooth" constitutes one of the only operations that achieved extensive publicity.[69] The plan of the operation, in which about two hundred combatants from the General Staff Reconnaissance Unit and the Kingfisher Unit were assigned to participate, was to raid a hospital in Baalbek where, according to the assessment, an Iranian physician had treated the captured Israeli soldiers, whose kidnapping had been one of the triggers for the war.[70]

The operation was launched on August 1, with Minister of Defense Peretz calling it "the operation that will change the face of history."[71] After four hours in Hezbollah territory, the forces returned without any Israeli casualties. Although this was not the first time that the IDF's special forces had reached Baalbek, this operation was deliberately "noisy."[72] Once it was discovered that the sought-after physician was not in the hospital, the remaining mission

65 Niccolò Petrelli, "The Missing Dimension: IDF Special Operations Forces and Strategy in the Second Lebanon War," *Small Wars and Insurgencies* 23, no. 1 (2012): 67.

66 Nahum Barnea and Shimon Schiffer, "War on Three Fronts," *Yedioth Ahronoth* August 4, 2006, p. 3 [Hebrew].

67 Kfir, *The Ground Trembled*, p. 181.

68 Alex Fishman, "Mission Impossible," *Yedioth Ahronoth,* October 27, 2006, pp. 10–11 [Hebrew].

69 Amir Rapaport, "March of Stretchers on the Streets of Tyre," *Maariv,* July 20, 2007, p. 12 [Hebrew]; Petrelli, "Missing Dimension," p. 64.

70 Petrelli, "Missing Dimension," p. 64.

71 Ofer Shelah, "A War as You Requested," *Maariv NRG*, January 17, 2009 [Hebrew].

72 Amit Cohen, Doron Nahum, and Felix Frisch, "120 km in the Rear of the Hezbollah," *Maariv*, August 3, 2006, p. 4 [Hebrew].

was to take as many captives as possible, to seize documents that might have intelligence importance, and to kill about twenty Hezbollah terrorists.[73]

The operation was labeled a success, but many argued that its achievements did not justify the risk involved.[74] Officers in the General Staff as well as retired senior officers believed that the risk had been too great for the purpose of such a mission, whose duration had been cast in doubt in advance.[75] According to their arguments, the operation's targets had not justified the deployment of such large forces, who were liable to become ensnared in an incident involving many casualties and even captives.[76] The former chief of staff Ya'alon also believed that "particular types of operations involve very high risk; therefore, you launch them only when the achievements they are supposed to accomplish are of strategic importance . . . I am not sure that the operation in Baalbek was not foolhardy."[77]

Notwithstanding the operation's modest achievements, the IDF launched a media campaign. The IDF spokesperson distributed photographs taken during the operation and they were published numerous times in the media,[78] while the operation's commander in the field, Col. Nitzan Alon, was sent to brief the journalists.[79] The political and military elite wanted to demonstrate achievements that would outwardly suggest an Israeli victory.

Launching a Large-Scale Ground Campaign toward the End of the War

On August 11, the prime minister decided in favor of launching a large-scale ground operation reaching the Litani River, despite the knowledge at that time that the United Nations Security Council was supposed to pass a resolution about a ceasefire.[80] The decision to launch the ground operation was strange, especially considering the assessments made during the preparatory

73 Rapaport, "March of Stretchers on the Streets of Tyre," p. 13.

74 Rapaport, *Friendly Fire*, p. 217.

75 Limor and Shelah, *Captives in Lebanon*, pp. 254, 258.

76 Harel and Issacharoff, *Spiderweb*.

77 Limor and Shelah, *Captives in Lebanon*, p. 258.

78 Kfir, *The Ground Trembled*, p. 192; Limor and Shelah, *Captives in Lebanon*, p. 255; Rapaport, *Friendly Fire*, p. 222.

79 Kfir, *The Ground Trembled*.

80 Halutz, *At Eye Level*, p. 462; Yaakov Katz, "Wadi Saluki Battle—Microcosm of War's Mistakes," *Jerusalem Post*, August 29, 2006.

discussions, which raised the possibility of hundreds of fatalities.[81] The minister of defense clarified that the ground operation would not improve the terms of the ceasefire but would create the impression that Israel took the final action during the war. Israel was not asking the international community to declare a ceasefire as a lifeline from an unsuccessful war; rather it wanted to be recognized as the side that was being asked to stop the fighting.[82]

The discussions in the IDF and within the political echelon about launching the operation focused heavily on the question of "staging the victory": How could the IDF instill the sense that it emerged victorious from the war, despite everything that had happened over the previous four weeks.[83] Harel Issacharoff described this well: "Just like Hezbollah, Israel is also searching now not only for an image of victory, but also a 'victory story,' an orderly description of the course of events, which will present the end of the campaign to the public as an Israeli triumph, which justifies the blood that was spilled and the houses that were destroyed."[84] Indeed, Chief of Staff Halutz argued during the cabinet meeting of August 9 that "the ground operation is needed for two reasons: in order to accomplish the mission of reducing the rockets, and secondly— because of the imagery. The IDF needs to and can operate on the ground and win."[85] The Winograd Committee report provides a basis for these statements, when it acknowledged that "Operation Change in Direction 11 was supposed to be a major, large-scale ground operation that would fundamentally change the reality in southern Lebanon and the imagery of the operation from a military perspective."[86] During his testimony before the Winograd Committee, Prime Minister Olmert argued that "if Maroun al-Ras had looked differently, if Bint Jbeil had looked differently, it could be that we would not have had to reach the point that we reached in the end."[87]

Others believed that launching the final attack had fundamentally been a mistake and should never had occurred in the first place, since—apart from the cognitive achievement—it could not have produced any strategic

81 Rapaport, *Friendly Fire*, p. 295.

82 Limor and Shelah, *Captives in Lebanon*, p. 311.

83 Harel and Issacharoff, *Spiderweb*, p. 398.

84 Avi Issacharoff and Amos Harel, "An Earthquake Soon," *Haaretz*, August 11, 2006 [Hebrew].

85 Limor and Shelah, *Captives in Lebanon*, p. 309.

86 Winograd Committee, *Second Lebanon War*, p. 387.

87 See Ehud Olmert's testimony before the Winograd Committee https://bit.ly/2BNAUkf.

achievement, particularly given the timing of its launch.[88] Thus, for example, Minister of Transportation Mofaz argued in an interview after the war that "with six hours [the time allocated for the operation], it is impossible to have sufficient time to accomplish a mission that was planned to take several weeks . . . the massive deployment of ground forces into Lebanon had not been a military and political necessity, but rather, was the outcome of frustration about the lack of achievements. In the IDF, they understood that you can accomplish achievements only by using ground forces."[89] According to Maj. Gen. (ret.) Danny Yatom, who had formerly headed the Mossad, the ground attack had no chance of producing a significant achievement, and, moreover, it was impossible to reach the Litani River in six hours.[90] The head of the research division at the Military Intelligence Directorate, Brig. Gen. Yossi Baidatz, also felt that the last-minute operation would not have any impact on Hezbollah. Baidatz also clarified his position in a letter that he sent to Olmert, Peretz, and Halutz.[91] Another senior officer who was opposed to the operation was the prime minister's military secretary, Maj. Gen. Gadi Shamani, who expressed to the prime minister that launching that operation at that stage had been pointless.[92] Even Maj. Gen. Ben-Reuven, who devised the "Mei Marom" contingency plan and constantly pushed for its implementation, argued that "the approval for the [Mei Marom] plan was not issued in time; there was already no chance to reach a full

88 Yair Ettinger and Amos Harel, "The Battle Was a Success, They Say in the IDF, But it is Unclear What the Objective Had Been," *Haaretz*, August 22, 2006 [Hebrew]; Yossi Ben-Ari, *The Second Lebanon War through the Perspective of the Press in Israel,* (Tel Aviv: Rothschild-Caesarea School of Communications, Tel-Aviv University, 2007), p. 24 [Hebrew]; Nahum Barnea, "The Final Days," *Yedioth Ahronoth*, January 25, 2008, p. 4 [Hebrew].

89 Nahum Barnea and Shimon Schiffer, "This is Not How You Wage a War," *Yedioth Ahronoth*, September 15, 2006, p. 4 [Hebrew].

90 Danny Yatom, *Confidant in a Secret* (Tel Aviv: Yedioth Ahronoth, Hemed Books, 2009), p. 431 [Hebrew].

91 Rapaport, *Friendly Fire*, pp. 321–322.

92 Schiff, "A Senior Officer in the Military Intelligence Directorate Warned the Prime Minister in Advance."

achievement."[93] The former chief of staff Ya'alon voiced extremely harsh criticism of the operation, calling it a "battle to save the leaders."[94] He said, "This operation was to achieve a media spin . . . its purpose was to achieve the missing victory picture . . . thirty-three soldiers were killed for a spin . . . you don't do such a thing. You do not send soldiers on a futile mission after the political outcomes have already been determined."[95]

It appears that the public pressure to launch an extensive ground operation, which would produce the desired achievements, is what tipped the scale: The results of a survey conducted for the *Haaretz* newspaper showed that only 28 percent of the public had expressed support for an immediate ceasefire, considering the limited achievements in the political arena. Furthermore, Yossi Ben-Ari's study found that the dominant trend in print journalism had been "to push the State into a battle" in order to achieve a victory, or at least, "an image of victory," the aim being to restore the eroded Israeli deterrence.[96]

Conclusion

During the Second Lebanon War, Israel invested considerable efforts in attempting to shape the public's cognitive perception, to convince it of the war's successes and achievements, and thus to increase the internal legitimization of the operation and of its casualties. As the war continued, there was an intensifying need to gain achievements that the public would perceive as significant. With this in mind, military operations were launched whose objectives were on a cognitive level; in many instances, however, these operations failed to create the desired cognitive perception of victory.

---

93 Lam, "The Contingency Plan Failure." Formulated prior to the Second Lebanon War, Mei Marom was a contingency plan that included wide-scale ground maneuvers in Lebanon. Although it was still in advanced stages of formulation, the plan was theoretically implemented in an exercise of combined forces, with an opening scenario similar to what took place in July 2006: a kidnapping in the Gaza Strip and then one in the north, followed by Katyusha rockets and escalation for several weeks. The Mei Marom contingency plan did not manage to pass the authorization process, and, thus, on the eve of the war, there was no updated and approved attack plan.

94 Ya'alon, *Long Short Road*, p. 210.

95 Ari Shavit, "Ya'alon: Soldiers Died for a Spin: The Leaders Need to Go," *Haaretz*, September 14, 2006 [Hebrew].

96 Ben-Ari, *Second Lebanon War through the Perspective of the Press in Israel*, p. 25.

The examples reviewed in this article were intended to illustrate the complexity of decision making and the tension between the need to gain achievements in war, including cognitive ones, and the risk of carrying out these operations. Internal legitimization played an important role in the decision makers' considerations, to the point that public pressure to gain significant achievements motivated the political echelon to launch a ground operation toward the end of the war, even though its strategic purpose had been doubted, especially given the imminent ceasefire.

The findings presented above indicate the conflicting pressures exerted by the public upon leaders of democratic countries during wartime: The public wants rapid and impressive achievements, while it also wants the number of casualties to be as low as possible. The decision makers strive to maintain a delicate balance between these two demands, but sometimes the deciding factor is the perception of the public's sentiment, which measures the war's objectives and achievements throughout the fighting vis-à-vis the number of casualties.

The Israeli leadership's concerns about casualties and its need for internal legitimization at times paradoxically led to the launch of operations involving risk to the soldiers. One can argue that considerations of internal legitimization, including considerations about the number of casualties—which are common mainly in democratic countries—are liable to negatively influence the decision makers' judgment during war.

Guidelines for the Management of Cyber Risks

Gabi Siboni and Hadas Klein

Cyber risk management is crucial to improving the level of organizational defense and preparedness for cyber events. This process is an important component in an organization's operational risk management and in its overall risk management. Organizations in several sectors within Israeli society are obligated to a process of managing cyber risks in accordance with the instructions of the regulator. The aim of this article is to examine the method of risk management, to propose guidelines for the management of cyber risks, and delineate the major stages of this process.

Keywords: Risk management, business continuity, cyber risks, cyberspace

Introduction

In May 2017, the media published reports about the theft of personal information of Kmart customers, marking the second time in three years that the data of Kmart shoppers had been stolen. Several small banks in the United States reported that they received warnings from credit card companies regarding a number of batches of stolen credit cards, which all had one thing in common: They were used to make purchases from the retailing giant Kmart. Given the reports in the media, Sears Holdings, the owner of Kmart, confirmed that some of its payment systems had been damaged by

Dr. Gabi Siboni is the head of the Cyber Security Program at the Institute for National Security Studies. Hadas Klein is a researcher in the Cyber Security Program at the Institute for National Security Studies.

hostile code. According to the company, advance detection failed to identify the code, but after detecting the cyber event, the malware was cleaned from the systems. Sears Holdings, however, did not address the question of how many of Kmart's 735 stores had been compromised by the event.[1]

The response of Sears provides additional evidence that preventing cyber events is critically important, even more so than the ability to identify and recover from them. This was especially significant in the case of Kmart, which was first attacked in October 2014 and has still not recovered; since the first cyber event, its sales have plummeted by more than 72 percent and its stock price has fallen by 88 percent.[2]

Addressing these attacks as a series of individual events as opposed to a systemic failure can be problematic, particularly when it results in insufficient treatment that should be done across the organization. The management of cyber risks and risks to supporting systems is meant to address systemic problems precisely of this kind. Kmart did not provide detailed information about the event, but involved parties have noted that even though the source of the problem may have been a component of the supply chain or employee negligence, it can be assumed that the root of the problem in both instances was the same: poor risk management, lack of inter-organizational transparency, and difficulty identifying the relationships between different systems.[3]

The management of operational and financial risks within organizations is a well-developed approach that is today widely implemented. In recent years, many organizations have also been applying this approach in managing computerized systems risks and cyber risks. This article seeks to provide those engaged in this work with guidelines and a methodology for conducting risk management in the cybersphere. It begins with a theoretical survey of the field of risk management and its benefits for organizations and then continues with a detailed proposal to implement in practice.

1 Brian Krebs, "Credit Card Breach at Kmart Stores. Again," *KrebsOnSecurity*, May 2017, https://krebsonsecurity.com/2017/05/credit-card-breach-at-kmart-stores-again.

2 Steven Minsky, "Kmart Cyber Breach: Another Failure in Risk Management," *LogicManager*, July 26, 2017, https://www.logicmanager.com/erm-software/2017/07/26/kmart-cyber-breach.

3 Minsky, "Kmart Cyber Breach."

The Theory of Risk Management

Risk management is a method that became a subject of study and research following World War II. The knowledge of this field originated with two books published in the mid-1960s that addressed the theory of risk assessment.[4] The process of risk management first began by examining market risk to defend against financial losses that could result from events and accidents. In the 1970s, it began to develop as a tool for managing the financial risks faced by financial institutions, banks, and insurance companies. Analysis of operational risks and liquidity risks appeared in the early 1990s.[5] Since then, risk management has become widely practiced within a variety of organizations, including commercial companies, airlines, state authorities, and so forth.

In the business world, risk management is conducted in many areas, including operational risk management; that is, assurance that the operational infrastructure of the organization will continue to function even if fundamental components should fail; financial risk management, including credit risk, currency risk, and market risk; and the management of risk related to regulation, law, or ethics.

The aim of the risk management process is to reduce the impact of irregular events on the organization. The process involves formulating risk scenarios that could detrimentally harm the organization; assessing the potential for damage should these scenarios occur; estimating the probability of the scenarios in question; prioritizing control measures for addressing scenarios based on their intensity, which is a combination of the impact of the risk and the probability of its being actualized; and finally, devising a plan to reduce risk. The life cycle of the risk management process typically consists of several stages, as discussed below.

4 R. I. Mehr and B. A. Hedges, *Risk Management in the Business Enterprise* (Homewood, Il: R. D. Irwin, 1963); A. Williams and M. H. Heins, *Risk Management and Insurance* (New York: McGraw Hill, 1964).

5 Georges Dionne, "Risk Management: History, Definition and Critique," *Risk Management and Insurance Review* 16, no. 2 (Fall 2013): 147–166.

Stage 1: Defining an Organization's Risk Appetite

The term "risk appetite" refers to the amount of general risk that an organization is willing to take in order to achieve its goals.[6] It expresses an organization's willingness to sustain high/low levels of exposure to risk and uncertainty in order to achieve its strategic goals. An organization's board of directors and management typically determine the risk appetite. It is a subjective process that is supposed to strike a balance between the potential returns that accompany the risk taking and the potential loss from it. Risk appetite frameworks provide the management with a clear picture of the desired risk and a perspective to balance between risk and return. An organization's risk appetite is not static; the management may request to change the level of risk it is willing to take according to conditions over the course of time.

Stage 2: Identifying Risk Scenarios

This stage involves identifying the risks by conducting research, which includes formulating risk scenarios based on the history of risks that were internal and external to the organization. This is done by surveying the organization's critical business processes, to understand which are most meaningful for the organization's functioning. These include examining processes of production, operations, and sales; surveying organizational assets that support these processes (such as manpower, computer infrastructure, machines, and so forth); analyzing the organization's exposure to risks that could have implications on its management, such as economic risks (for example, a slowing economy) and how these risks can affect the company's sales; analyzing sectoral risks, such as the impact of Israel's security situation on the foreign tourism sector; and finally, examining the legal and regulatory requirements, such as the impact of safety laws, building laws, and the like.

Stage 3: Analyzing Risk Scenarios

Risk is defined as the probability of a harmful event occurring, combined with the outcome of the event itself. Risk therefore is the product of two parameters: the probability that a specific scenario will occur and the anticipated impact of the damage if the scenario is realized. The result of multiplying these two measures is known as inherent risk i.e., the level

6 "Principles for an Effective Risk Appetite Framework," *Financial Stability Board*, November 18, 2013.

of the untreated risk. Identifying and analyzing risk scenarios is based on research, which includes examining similar scenarios in the history of the company and elsewhere, providing expert opinions, assessing previous risk management/survey reports, financial reports, legal proceedings, information regarding insurance claims, and so forth.

The intensity of the damage is assessed according to parameters of direct and indirect damage resulting from a scenario of harm to the organization. Direct damage can result, for example, from disrupting an organization's operational continuity as a result of disabling the systems or being unable to engage in production as planned. Examples of indirect damage might include injuring the organization's reputation as a result of being unable to meet its obligations, legal claims, and so forth.

Stage 4: Formulating a Plan to Reduce Risk

Control measures are tools and processes that organizations use to reduce risk. An organization's control system consists of all the tools that are part of an organization's work processes in relation to the objects of risk. An organization cannot run effectively without a systematic and proper system of controls.

The types of control measures that operate within an organization can be divided into several categories:

- *Preventative controls*—designed to prevent causing a failure, including changes to the organization's mode of operation. For example, a production process may be found to be excessively dangerous, and as a result, the management may decide to refrain from employing it.
- *Diversion tactics*—intended to shift the impact of the failure to an external party, such as a subcontractor or an insurance company.
- *Detective controls*—designed to detect undesired actions that have already taken place, which then enables the organization to rectify them after their occurrence. An example is producing a report of irregularities in order to analyze and monitor irregular actions.
- *Corrective controls*—intended to rectify undesired actions after their occurrence. One example is the automatic reconstitution of data after a computer system crashes.
- *Compensative controls*—aimed to provide a response where the existing controls are not sufficiently strong enough.

Stage 5: The Analysis of Residual Risk

Residual risk is risk that remains after applying the risk reduction plan. After implementing the controls, the level of residual risk should be lower than the level of the inherent risk of the event analyzed. In addition, the level of residual risk must be within the limits of the designated risk appetite. If the residual risk is unacceptable (too high), additional control measures must be implemented to lower the residual risk to an acceptable level, as determined by the management in its definition of risk appetite.

The Importance of Cyber Risk Management

The rapid pace of technological change, the increasing number and availability of digital services—interfacing with the old system—and the growing need for lines of communication with suppliers has created a breeding ground for developing cyber threats, thus exposing many organizations to critical cyber risks. The past decade has also witnessed a steady increase in the number of threat factors, in terms of ability, availability, attack tools, and attack groups. As a result, it has been only natural to manage cyber risks with methods of risk management; nonetheless, we still have a long way to go until these methods are routinely implemented.[7]

Cyber risks are part of both the operational and the overall risk management in an organization. According to a survey conducted by Deloitte Israel in 2017, the number of organizations managing cyber risks has increased significantly.[8] Some 60 percent of the major companies in Israel collect and analyze information in order to obtain an updated picture of cyber threats. The survey also indicates that more than 50 percent of the large companies in the Israeli economy maintain a risk management framework and implement a corporate cyber defense policy, while a comparable number conducted a cyber risk survey in the year that preceded the report. Although these figures are higher than average within the Israeli economy as a whole, there is still room for improvement.

Adopting a risk management approach in the field of cybersecurity has a number of advantages:

---

7 "The Israeli Market and Cyber Threats: A Situation Assessment, 2017," *Deloitte Israel*, 2017, https://www2.deloitte.com/content/dam/Deloitte/il/Documents/risk/Deloitte_Cyber_Infographic1.2.pdf.

8 "The Israeli Market and Cyber Threats: A Situation Assessment, 2017."

- *Financial* —Optimizing a cyber defense system and developing an information security policy can prevent not only direct losses, such as monetary theft, but also indirect losses, such as damage to reputation. It can also prevent fines for non-compliance with legal and regulatory requirements. For example, violation of the European Union's international regulations for the protection of data (the General Data Protection Regulation) results in administrative fines of up to €20 million, or up to 4 percent of an organization's annual turnover, whichever is greater.[9] A cyberattack can also impact a company's stock price by dealing a severe blow to customer trust and/or damaging its reputation and brand name.
- *Strategic* —Appropriately addressing the cyber challenge with an optimal cyber defense system enables the organization to clearly understand its exposure to cyber risks. This affects the level of trust among the interested parties and investors in the organization as well as the organization's ability to achieve its goals.
- *Legal* —In many countries, an organization's protection of its information and its digital assets are defined by law as being the responsibility of the organization's managers and board of directors.
- *Operational* —A cyber event may affect a variety of operational elements, including the supply chain, production pricing, manpower, and so forth. For example, a cyber event that damages the lines of communication with company suppliers can result in substantial disruptions to the production process.
- *Business Continuity*—An improved capacity to handle cyber events has a direct result on an organization's ability to maintain business continuity or at least to minimize the time it takes to resume work.

The challenge of cybersecurity is often seen as being within the purview of information system personnel, who also hold the key to the solutions. Today, however, it is clear that cybersecurity is not a problem that can be resolved by using technological tools alone; rather, it is a comprehensive challenge that encompasses people, organizational processes, technology, and organizational policy. These and other elements are extremely important to the organization's overall security, stability, and strength.

9 Section 83 of Regulation (EU) 2016/679 of the European Parliament and of the European Council, April 27, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

Cyber Risk Management

Cyber risk events can disrupt an organization's proper and secure activity, can cause failure to provide service, expose business or customer information, delete and disrupt data, and so forth. Damage potential is a standard aspect of risk management. In the cybersphere, the potential for damage is manifested not only in damaging the information within the context of the triad of confidentiality, integrity, and availability but also in other aspects, such as reputation, law and regulation, and business continuity.

In recent years, several regulatory directives relating to cyber risk management have been issued. One example is the Bank of Israel's Proper Conduct of Banking Business Directive No. 361 regarding cyber defense management.[10] This directive requires the banks in Israel to manage their cyber risks in order to reduce the probability of their being realized. Defining the methodology of cyber risk management requires organizations to prepare risk scenarios and analyze their systems of protection.

The instructions of Israel's Ministry of Finance stipulate that institutional bodies in Israel must assess their cyber risks using the following measures: identifying processes, systems, and information assets; mapping the risks posed to processes, systems, and information assets; framing the inherent risks; mapping and assessing the control measures for minimizing these risks, including the impact of the control measures on the risks themselves; and finally, assessing the residual risk according to the effect of the control measures that were implemented.

To implement these principles, it is recommended to act according to the risk scenario—based on the organization's processes and the information assets that are to be protected—and to continue defining the cyber risk scenarios to which the organization is vulnerable. It is also recommended to assess the inherent risk should the scenario be realized, as well as to analyze the maturity of the cyber control system by evaluating the extent of its assimilation, and then to consider the effectiveness of the organization's available cyber controls. Finally, it is recommended to evaluate the residual risk and the breaches in defense and to prioritize formulating a work plan designed to meet these gaps.

10 Bank of Israel, Circular 2457-06-H, Cyber Defense Management, March 16, 2015, http://www.boi.org.il/en/BankingSupervision/LettersAndCircularsSupervisorOfBanks/Curculars/h2457_en.pdf.

Defining Risk Scenarios

The method of defining risk scenarios begins with analyzing the organization's critical business processes, in addition to their supporting digital systems and assets. It then continues with formulating possible cyberattack scenarios. This stage is based on intelligence gathering and analyzing attack trends and potential cyberattackers. In addition, unintentional technological fault scenarios should also be analyzed. The attack scenarios should be mapped onto the critical processes and their supporting systems.

The critical processes and their supporting digital systems and assets are analyzed by applying the Business Impact Analysis (BIA). BIA is part of a broad toolbox meant to contribute to business continuity and help the organization recover as quickly as possible after an event. BIA is part of the recovery plan as it can help estimate the damages caused and the relative importance of the different parts of the organization. Organizational BIA documents sometimes fail to relate to the various aspects of the cybersphere, such as confidentiality and informational integrity. Documents that do not address specific cyber elements should be updated accordingly. The BIA and the organizational cyber defense strategy document should provide a prioritized list of the digital assets that are designated for protection. In this framework, it is important to define the principles and the aims of defense, as determined by the organization's board of directors, the regulators, and other parties of interest.

Contending with possible cyberattack scenarios requires an assessment of the organizational cyber risks as they relate to a number of points: Who are the parties that could have an interest in attacking the organization? What are their capabilities and the tools at their disposal? Who have they attacked in the past and in what manner? This assessment should rely on a preliminary process of intelligence gathering, including analysis of attack trends, potential attackers, and their capabilities.

Intelligence gathering focused on the needs of the organization should define the relevant components of information to be gathered. This action is usually referred to as EEI (essential elements of information). EEI defines the range of relevant sources of information and the focus areas for information gathering. For example, a banking organization in Israel should concentrate its intelligence gathering on threats to the banking industry by criminal

organizations, enemies, and activist groups that could take action against a specific economic policy or against "global capitalism."

The information gathered serves two primary goals. The first is to continuously update the threats, which serves the organization in assessing the situation and in providing rapid and focused responses to new threats. The second is to formulate risk scenarios with which the organization could be forced to contend, while also noting relevant parameters for quantifying the threat, including the probability of the event, the extent of damage, and so forth. The sources of information for intelligence gathering include commercial information services (in accordance with EEI), available free sources, cooperative endeavors, and information sharing with relevant parties (such as sectoral cooperation centers), CERT (Computer Emergency Response Team) and other parties, and finally, parties that provide the organization with guidance.

The Assessment of Inherent Risk

The process of assessing inherent risk is conducted in two stages: weighing the damage potential in the event that a risk scenario is realized, and evaluating the probability that the scenario will take place. Assessment of the damage potential of each scenario should be done in consultation with commercial parties. They can estimate the extent of economic loss for each scenario while analyzing the risks to strategic business assets as defined by the organization and important to protect. In addition to the direct damages, indirect damages—such as exposure to legal claims, sanctions, damage to reputation and functional continuity—should also be considered.

A number of measures are used to determine the probability of a scenario being realized. The first is the realization of a similar scenario in a comparable organization in the past. However, due to the difference among cyberattacks and the existence of an extremely wide variety of attack scenarios and events, we cannot rely solely on this measure. It is therefore possible to use two additional measures. The first one reflects the cyber intelligence team's subjective assessment of the probability of a risk being realized, using a ranking of 1–5 (with 5 indicating the highest likelihood of occurrence). The second measure is the level of structural exposure, or how easy it is to attack the assets as described in the scenario. Structural exposure is determined by the different attributes of the organization's internal technological

environment, which include the number of interfaces, the number of users, internet access, communications equipment, connectivity between stations, and so forth. Each attribute is given a value, which ranks the technological environment's level of exposure to cyberattack. These values are also based on a scale of 1–5, with 5 indicating the most easily attacked. For example, the more internet access points an organization has, the easier it is to attack it. An organization with one point of access to the internet, therefore, will receive a ranking of 1, whereas an organization with dozens or hundreds of internet access points will receive a ranking of 5. Each attribute is similarly assessed. To calculate the level of structural exposure, an adjusted calculation of the average scores of the various parameters is conducted.

The likelihood of a risk (RL) being realized is calculated by the following formula:[11]

$$RL\ (Risk\ Likelihood) = \frac{RE\ (Risk\ Exposure) \times AS\ (Analyst\ Score)}{5}$$

when RE is the score for structural exposure, and AS is the score given by the intelligence investigator to the probability of the risk being realized. The purpose of dividing by 5 is to standardize the probability for values between 1 and 5.

Inherent risk (IR) is calculated as follows:

$$IR\ (Inherent\ Risk) = \frac{RL\ (Risk\ Likelihood) \times RI\ (Risk\ Impact)}{5}$$

when RL is risk likelihood, and RI is risk impact.[12] The purpose of dividing by 5 is to standardize the probability for values between 1 and 5.

The analysis of systems that support critical processes in an organization, the gathering of intelligence and its analysis for threats, and the completion of risk analysis enable the assessment of the organization's critical cyber risks. Below is an example:

11 All values are ranked from 1–5.

12 The approach to calculating inherent risk presented in this article is one of a number of existing approaches. It is presented here for the purpose of example.

Title of the Threat	The Title of the Threat for the Sake of Establishing a Common Language
Cause of the Threat	The cause of the threat based on the intelligence gathered.
Route of Attack	The route of the threat being realized based on the organization's intelligence and technological information.
Critical System Affected	From the list of systems that support critical processes.
Probability	Assessment of the probability of the scenario's realization.
Damage	Assessment of the potential damage stemming from realizing the scenario.
Inherent Risk	Measure of the inherent risk as calculated using the inherent risk equation.

Assessment of the Maturity of Cyber Defenses

Controls in the cyber realm can be classified into three primary categories:

1. *Preventative control measures,* which are meant to assist in monitoring and supervising data and activities and in preventing errors, oversights, and intentional damage. Examples of control measures in this category include the separation of positions and permissions, entry controls, and the gathering and analysis of cyber intelligence.
2. *Detective control measures,* which assist in identifying irregularities. Examples of control measures in this category include systems for the detection of anomalies in the users' behavior, such as a user working at unreasonable hours and performing actions that are not part of the usual work of his or her position.
3. *Corrective control measures*, which assist primarily in restoring the previous situation and routine (for example, back-up and reconstitution processes) and in improving defenses.

The overall control system should be adapted to meet the needs of the organization. Today, there are a number of standards and directives that define a general control system structure. Examples can be found in the recommendations of the National Institute of Standards and Technology (NIST), which provides guidance for US federal bodies,[13] and the Federal Financial Institutions Examination Council (FFIEC), which sets standards for the banking sector in the United States.[14] Organizations can also make use of the cyber defense doctrine that was written by Israel's National Cyber

13 "NIST Cybersecurity Framework," *NIST*, https://www.nist.gov/cyberframework.

14 "Cybersecurity Assessment Tool," *Federal Financial Institutions Examination Council (FFIEC)*, https://www.ffiec.gov/cyberassessmenttool.htm.

Directorate.[15] Assessing the control measure maturity is done individually by analyzing two parameters: first, the extent of the control's implementation and second, its effectiveness.

Assessing the control maturity requires conducting interviews with technological personnel within the organization and with other parties, such as a risk management unit (if such a unit exists within the organization). A table should be prepared for each control measure, reflecting its own unique scoring. A scale assessing the implementation of the control measure within the organization needs to be defined. This analysis is done according to the unique parameters of each control measure, using a scale of 1–5, with 5 indicating maximum implementation. The following table provides an illustrative example analyzing the control measure of employee awareness of cyber risks:

Assessment of Assimilation of Control Measure	Score
There is no process of building employee awareness.	1
There is a basic process of awareness building, including instructional sessions, fliers, organizational portal.	2
An advanced process of awareness building has been implemented, including general exercises.	3
An advanced organizational process has been implemented, including performance control and measurement.	4
An advanced organizational process has been implemented, in addition to an external process aimed at building business partners' awareness of cyber risks.	5

It is also necessary to assign a value to each control measure indicating its importance in the organization's overall defense system. The values range from 1–5: The greater the control measure's importance to the defense system, the higher value it is assigned. At the end of the control assessment process, the maturity score can be determined using the following matrix:

15 "Cyber Security Methodology for Organizations," *National Cyber Directorate, Prime Minister's Office* [Hebrew], https://www.gov.il/he/Departments/policies/cyber_security_methodology_for_organizations.

$CM =$

CA Assimilation of Control	*CI* Control Importance 1	2	3	4	5
1	5	3	2	1	1
2	5	3	2	2	2
3	5	4	3	3	3
4	5	4	4	4	4
5	5	5	5	5	5

Control maturity (CM) is a function of control importance (CI) and the extent of the control's assimilation within the organization (CA). It is determined in accordance with the values of the matrix.

Control maturity scores are determined according to the values that appear in the matrix. In this way, a preferred plan can be set up for handling the control measures. The lower the control maturity score is, the higher priority it should be given. This means that the control measures at the top of the list will be optimal to improving the overall system of defenses.

The matrix values deal with extreme situations in the following manner: It is not necessary to invest resources to address a control measure that has a score of 1 (low) in importance; therefore, the control maturity value for all controls with an importance of 1 is 5. In addition, investing in a control measure with an implementation score of 5 (maximum) is unnecessary, and therefore the control maturity value for all control measures with an implementation level of 5 is 5. It is also important to consider the costs of addressing control measure. For example, a control measure with installation and maintenance that is expensive and eats up a significant portion of the budget of the defense system is not necessarily effective, even if defense tops the list of priorities. In such a case, normalization can be conducted, reflecting the relative cost of the control.

Analysis of Residual Risk

Residual risk indicates the potential of damage that could be caused to an organization as a result of a cyber event that occurs after implementing the existing control measures. For the organization to contend with cyber risks, it must assess the residual risk for each individual scenario, as identified at earlier stages of the process. Residual risk (RR) is calculated using the following formula:

$$RR\ (Residual\ Risk) = IR\ (Inherent\ Risk) - w \times CS\ (Control\ Score)$$

when IR is inherent risk, CS is controls score (the quality of available controls), and *w* is a control score coefficient. It is often acceptable to assign a coefficient when calculating the residual risk so that the quality of the available controls is reduced by a certain percent, in order to benefit from a higher level of confidence in the residual risk. For example, it could be decided to make use of a controls score that is 30 percent lower than that calculated, which would require using w=0.7 in the formula.

Calculating residual risk requires determining the overall score of the cyber defense system for the scenario in question. This is done using the following formula:

$$OCM\ (Overall\ Control\ Maturity) = \frac{\sum_{i=1} CM_i\ (Control\ Maturity)}{n}$$

when the Overall Control Maturity is the average of *n* Control Maturity scores for the scenario in question. The residual risk for each scenario is calculated using the following formula:

$$RR\ (Residual\ Risk) = IR\ (Inherent\ Risk) - w \times OCM\ (Overall\ Control\ Maturity)$$

when IR is inherent risk, CS is controls score, and w is the CS coefficient.

Now, the organization can assess whether the residual risk is compatible with the risk appetite as defined by the organization's management. In the event of disparities, it will be necessary to return to the stage of control prioritization and to formulate a work plan aimed at improving the system of defenses or alternatively, to reduce dangerous activity in the cybersphere.

Conclusion

The aim of this article was to provide guidelines for the management of cyber risks, based on the basic theory of the discipline of risk management that has been evolving since the 1960s. The article presents one approach to the proposed process. Although other approaches exist, almost all rely on the theoretical basis of risk management.

Managing cyber risks is a critical component in managing an organization's cybersecurity systems in addition to other elements, such as penetration tests. This process enables the organization to assess the level of risk it faces, to

methodically define the organization's means of defense, and to determine whether the level of exposure to risk is compatible with that defined and stipulated by the board of directors, the organization's management, and the various interested parties.

Implementing the guidelines described above are not a guarantee for preventing cyber events. They will, however, ensure that those responsible for the organization's defense systems will acquire a deeper understanding of the cyber risks with which they must contend. Thus, implementing the guidelines can go a long way in reducing the risks that an organization faces within the framework of its business needs. According to expert assessments, the systemic problem discovered in the Kmart corporation during the cyberattacks discussed above was due to poor implementation of risk management processes.[16] Implementing a systematic and orderly risk management process can help reduce an organization's exposure to risks, as well as diminish the reputational and financial damage that may result from events of this kind.

16 Minsky, "Kmart Cyber Breach."

Securing Critical Supply Chains: Strategic Opportunities for the Cyber Product International Certification (CPIC™) Initiative

Paul Stockton

China, Russia, and other potential adversaries are increasing their efforts to corrupt the supply chains upon which the electric grid and other infrastructure sectors depend. Valuable initiatives are underway to strengthen supply chain risk management (SCRM). Yet, despite these measures, the US intelligence community warns that the growing scale and sophistication of attacks on the supply chain "are placing entire segments of our government and economy at risk."[1] Similar challenges confront Israel, the United Kingdom, and other US security partners.

At present, infrastructure owners and operators lack a compressive, stakeholder-driven process to certify that crucial hardware and software products are even minimally scrubbed of malware and other means of adversary exploitation. Establishing such a certification process contribute enormously to cyber resilience,

Dr. Paul Stockton is the managing director of Sonecon, LLC, and a former US assistant secretary of defense for Homeland Defense and America's Security Affairs. Robert Denaburg, a senior analyst at Sonecon, performed research for the report. The findings and recommendations in this article are solely those of the author and do not necessarily reflect the views of the Department of Defense or any other US government agency.

1 National Counterintelligence and Security Center, "Supply Chain Risk Management: Intelligence.Gov Background Paper," March 2017, p. 2, https://www.dni.gov/files/NCSC/documents/products/20170317-NCSC--SCRM-Background.pdf.

especially if government agencies can provide threat information and other forms of support for the initiative.

The Cyber Product International Certification (CPIC) initiative proposed by the Electric Infrastructure Security (EIS) Council will help meet these challenges. CPIC could add even greater value for infrastructure resilience by including measures to certify products against intentional electromagnetic interference (IEMI).

Keywords: Cyber, threats, supply chain, OT, energy, CPIC

The Scope and Severity of the Threat

The risks posed by Russian and Chinese hardware and software to infrastructure resilience (and to national security) have garnered intense government scrutiny in recent months.[2] However, products sold by ZTE, Huawei, and Kaspersky Labs constitute only the publicly visible "tip of the iceberg" of hostile efforts to corrupt supply chains and enable potential adversaries to establish persistent presence in US and partner networks.

In the Department of Homeland Security's May 2018 "Cybersecurity Policy," the department warns that the growing connectivity of modern infrastructure sectors and services introduces new vulnerabilities and "opens the door to potentially catastrophic consequences from cyber incidents."[3] This is attributed in part to a reliance on increasingly global supply chains and the rapidly expanding number of internet-connected devices, which—without countervailing innovations that emphasize improved security and resilience—will continue to intensify supply chain risk management (SCRM) challenges.[4] Despite the current array of public and private sector programs to mitigate and counter supply chain threats, "the evolution of

2 See, for example, Danny Lam and David Jimenez, "US' IT supply chain vulnerable to Chinese, Russian threats," *The Hill*, July 9, 2017, http://thehill.com/blogs/pundits-blog/technology/341177-us-it-supply-chain-vulnerable-to-chinese-russian-threats; Joseph Marks, "Chinese Telecoms Could Join Kaspersky On Government wide Banned List," *Nextgov*, February 13, 2018, http://www.nextgov.com/cybersecurity/2018/02/chinese-telecoms-could-join-kaspersky-governmentwide-banned-list/145960.

3 Department of Homeland Security, "Cybersecurity Strategy," May 15, 2018, p. 1, https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf.

4 Ibid., pp. 22–23.

directed, sophisticated and multifaceted threats threatens to outpace our countermeasures."[5] Given the current threat environment and global supply chain trends, "cyber SCRM is not optional."[6]

While adversaries cannot remotely insert and exploit electromagnetic vulnerabilities in the same way they can with cyber weapons, a number of risks also exist. For example, adversaries could introduce components that are faulty or particularly susceptible to electromagnetic threats into infrastructure supply chains. Adversaries could also attempt to capitalize on known electromagnetic vulnerabilities in widely-deployed components, augmenting the potential damage caused by an electromagnetic attack.

Threats to global supply chains are multifaceted, and several factors and trends are intensifying these threats. This intensification of supply chain threats pose a number of challenges for successfully mitigating them as well as an imperative to do so.

1. Increasing number of threat vectors

Adversaries continue to find innovative ways to target, corrupt, and exploit supply chains. Indeed, the increasing global complexity of supply chains and intensification of adversarial threats have amplified the risk that suppliers could intentionally or unintentionally introduce compromised hardware, software, or firmware into a system or network.[7] New information technology (IT) initiatives such as cloud computing and the Internet of Things (IoT) have also expanded the cyber supply chain attack surface,[8] increasing the number of possible infiltration points that adversaries can target and creating additional challenges for infrastructure owners and operators in securing their supply chains.

Adversaries are seeking opportunities to corrupt every point in the global supply chains that support US infrastructure. Risks exist at each stage: design,

5 "Supply Chain Risk Management: Intelligence.Gov Background Paper," p. 2.

6 National Institute of Standards and Technology, "Best Practices in Cyber Supply Chain Risk Management," n.d., p. 1, https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-SCRM-Business-Case.pdf.

7 Ibid., p. 1.

8 Jon Oltsik, "Protecting the Cyber Supply Chain," *Cipher Brief*, December 6, 2015, https://www.thecipherbrief.com/article/protecting-cyber-supply-chain.

manufacturing, integration, deployment, and maintenance.[9] Adversaries may insert vulnerabilities into the supply chain themselves, or can potentially capitalize on latent, inherent vulnerabilities yet to be addressed by security practitioners.[10]

Even if a vulnerability does not exist in the initial development, adversaries can insert them at any point in the life cycle of a system.[11] This includes software updates or vulnerability-correcting "patches" for IT or operational technology (OT) systems which can upload malicious code into a system, or insert malignant firmware for exploitation at a later date.[12] The frequency with which system operators apply software updates creates multiple opportunities for adversaries to compromise systems long after the design stage.

Adversaries may also compromise the hardware that utilities install in their operating systems. For example, a Defense Science Board (DSB) report noted numerous potential vulnerabilities associated with supply chain compromise of microelectronics. While the DSB report focuses on weapons systems, similar microelectronics are increasingly present in every infrastructure sector. These microelectronics "will inevitably contain latent vulnerabilities" that may be discovered only years after the product enters into service—if at all—and potential effects range from system degradation to system failure.[13]

Software updates are especially prone to hostile efforts to gain persistent access to counter-intelligence networks, which adversaries could later use to launch disruptive attacks on infrastructure operations. For example, the Russian Dragonfly campaign initially targeted "peripheral organizations such

9 National Counterintelligence and Security Center, "Supply Chain Risk Management: A Framework for Assessing Risk," February 2013, p. 2, https://www.dni.gov/files/NCSC/documents/products/SCRM_Framework_for_Assessing_Risk_White_Paper.pdf.

10 Public-Private Analytic Exchange Program, "Identifying and Mitigating Supply Chain Risks in the Electricity Infrastructure's Production and Distribution Networks," 2016, p. 4, https://www.dni.gov/files/PE/Documents/Electricity-Infrastructure-Summary.pdf.

11 Defense Science Board, "Task Force on Cyber Supply Chain," February 2017, p. 1, https://www.acq.osd.mil/dsb/reports/2010s/1028953.pdf.

12 The Public-Private Analytic Exchange Program, "Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector: Recognizing Risks and Recommended Mitigation Actions," 2017, p. 12.

13 Defense Science Board, "Task Force on Cyber Supply Chain," February 2017, pp. 1–2.

as third-party suppliers with less secure networks," using them as staging targets to pivot to intended victims.[14] ICS cybersecurity firm Dragos, Inc. also recently profiled a threat actor that has targeted ICS networks, through the use of watering hole attacks to steal credentials and gain access to compromised victims' networks and machines.[15]

2. Covert ownership and globalization of supply chain vendors

Supply chains are becoming increasingly global. As supply chains become ever more intricate and international, the most capable adversaries "can access this supply chain at multiple points, establishing advanced, persistent, and multifaceted subversion."[16]

Ownership, control, and/or influence of points along global supply chains by malicious governments or government-affiliated corporations are particularly concerning. Software and firmware code is developed by suppliers in many countries, which "opens up plenty of opportunities for US adversaries, such as Russia and China, to sneak a hackable vulnerability into those systems that those nations' intelligence services can later exploit."[17] Similar concerns apply to the potential for adversaries to introduce components that are particularly vulnerable to electromagnetic threats into supply chains.

China also dominates the global capacity for IT-related assembly and manufacturing.[18] Many of the hardware products in infrastructure networks likely contain products manufactured in China, which could expose them to potential contamination. As evidence of this potential threat, intelligence officials and legislators raised concerns at a recent congressional hearing about Chinese penetration in the telecom sector—particularly of potential

14 United States Computer Emergency Readiness Team, "Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," *Department of Homeland Security*, last updated March 16, 2018, https://www.us-cert.gov/ncas/alerts/TA18-074A.

15 "CHRYSENE," *Dragos, Inc.,* May 17, 2018, https://dragos.com/blog/20180517Chrysene.html.

16 "Supply Chain Risk Management: Intelligence.Gov Background Paper," p. 1.

17 Joseph Marks, "DHS to Scrutinize Government Supply Chain for Cyber Risks," *Nextgov*, February 14, 2018, http://www.nextgov.com/cybersecurity/2018/02/dhs-scrutinize-government-supply-chain-cyber-risks/145998/.

18 Lam and Jimenez, "US' IT supply chain vulnerable to Chinese, Russian threats," *The Hill*.

equipment contracts with US government and industry.[19] The United States also banned the use of the Russian firm AO Kaspersky Lab's products from all federal information systems, citing security concerns.[20] Adversaries then could leverage system access for nefarious attacks.

Moreover, potential adversaries are already attempting to subvert SCRM initiatives and will likely do so successfully in the years to come. A prime example is Huawei Technologies. The Chinese ICT firm is a member of several cybersecurity organizations with SCRM-focused initiatives, including the Open Group (and their Open Trusted Technology Provider™ Standard (O-TTPS) Certification Program)[21] and SAFECode (and their Fundamental Practices for Secure Software Development).[22] In addition to direct supply chain threats, it is expected that SCRM initiatives themselves will become potential sources of adversary infiltration efforts.

3. Opacity and complexity of supply chains

As supply chains become more international, they are also becoming increasingly complex. The globalization process has been characterized by "a complex web of contracts and subcontracts for component parts, services, and manufacturing extending across the country and around the world," and the multiple layers and networks of suppliers are frequently not well understood.[23] The National Institute of Standards and Technology, a leading SCRM stakeholder, warns that it is becoming increasingly difficult to vet supply vendors and providers. Indeed, many companies find it challenging to

19 Marks, "Chinese Telecoms Could Join Kaspersky On Government-wide Banned List," *Nextgov*.

20 Department of Homeland Security, "Notification of Issuance of Binding Operational Directive 17-01 and Establishment of Procedures for Responses," *Federal Register* 82, no. 180, September 19, 2017, p. 43782, https://www.federalregister.gov/documents/2017/09/19/2017-19838/national-protection-and-programs-directorate-notification-of-issuance-of-binding-operational.

21 "Standard Open Group Membership," *The Open Group*, last updated June 5, 2018, http://reports.opengroup.org/membership_report_all.pdf.

22 "Members," *SAFECode,* https://safecode.org/members/.

23 "Supply Chain Risk Management: Intelligence.Gov Background Paper," p. 1.

vet supply chain partners beyond the first tier.[24] However, many infrastructure owners and operators depend on a "complex, globally distributed, and interconnected supply chain ecosystem" for products and services, which contain multiple tiers of outsourcing and diverse distribution routes.[25] Meanwhile, adversaries can operate through numerous front companies, organizations, and individuals to hide their presence, obfuscating efforts to discover and counter their actions.[26]

Given the increasing number of vendors and third-party providers upon which power companies rely, "utilities often find it difficult to ensure supply chain integrity."[27] It is possible that potentially compromised products could make their way into infrastructure systems without system owners' knowledge.

4. Convergence of information and operational technology networks

The growing convergence between IT and OT systems increases the potential risks and consequences of a cyberattack. OT systems such as Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS) are increasingly prevalent in infrastructure systems. And while these OT systems previously operated on a separate network, segmented from IT networks, the two are increasingly converging.[28] This is creating additional vulnerabilities and increasing systems' attack surfaces. More concerning, however, is that compromised OT systems—especially on a large scale—can have direct physical (and potentially catastrophic) consequences for infrastructure.

---

24 National Institute of Standards and Technology, "Best Practices in Cyber Supply Chain Risk Management: Vendor Selection and Management," n.d., p. 1, https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-SCRM-Vendor-Selection-and-Management.pdf.

25 "Cyber Supply Chain Risk Management," *National Institute of Standards and Technology,* last updated April 16, 2018, https://csrc.nist.gov/Projects/Supply-Chain-Risk-Management.

26 Ibid., p. 2.

27 Mission Support Center, Idaho National Laboratory, "Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector," August 2016, p. 15, https://bit.ly/2G4OQrH.

28 The Public-Private Analytic Exchange Program, "Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector," p. 4.

Ongoing Industry and Government Progress

Valuable and rapidly-growing SCRM initiatives are underway. Indeed, such initiatives are growing so rapidly that no comprehensive, up-to-date survey of these activities exists. The section that follows provides an initial attempt to offer such a survey. The list is surely not exhaustive, as some initiatives will undoubtedly be overlooked. Nevertheless, the section highlights many of the most important ones.

These SCRM efforts, which may come in the form of standards, best practices, and other regulatory measures, all focus on the same goal: "identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of IT/OT product and service supply chains."[29] SCRM initiatives should address "the entire life cycle of a system (including design, development, distribution, deployment, acquisition, maintenance, and destruction) as supply chain threats and vulnerabilities may intentionally or unintentionally compromise an IT/OT product or service at any stage."[30]

Many of the initiatives examined below assess and attempt to mitigate supply chain risks, sometimes for a particular sector or subset of infrastructure. The section first examines the electricity subsector initiatives. The next subsections outline SCRM initiatives that are multi-sector in nature, along with a new—and potentially very promising—initiative led by Siemens.

Energy Sector Initiatives

The energy sector, and especially the electricity subsector, plays a critical role in enabling all other infrastructure sectors. Threats to this sector are particularly acute, spurring both industry and government efforts to address the multitude of associated challenges. However, efforts to define requirements and further research and development to secure the supply chains for grid technologies is lagging, despite knowledge of adversarial threats and increased risks due to globalized supply chains.[31] Nevertheless, some important initiatives are underway which may form the basis of future efforts.

---

29 "Cyber Supply Chain Risk Management," *National Institute of Standards and Technology.*

30 Ibid.

31 Public-Private Analytic Exchange Program, "Identifying and Mitigating Supply Chain Risks," p. 2.

1. Department of Energy (DOE)

As the sector-specific agency (SSA) for the energy sector, DOE is working to address cyber supply chain vulnerabilities. The department's "Cybersecurity Procurement Language for Energy Delivery Systems" guidance, developed in partnership with industry, provides utilities with "strategies and suggested language to help the US energy sector and technology suppliers build in cybersecurity protections during product design and manufacturing."[32]

DOE also released its "Multiyear Plan for Energy Sector Cybersecurity" in March 2018. Among the plan's goals and objectives is the imperative to "reduce critical cybersecurity supply chain vulnerabilities and risks."[33] To do so, DOE plans to:

> *Identify actions the federal government can take to reduce supply chain risk*: DOE will work with federal partners to identify and take appropriate actions to mitigate supply chain cybersecurity risks and facilitate the building of trust between owners and operators and energy sector ICS manufacturers.
>
> *Develop an energy delivery systems (EDS) testing and analysis laboratory:* As threats continually evolve and new vulnerabilities are discovered and targeted by adversaries, national capabilities are needed to evaluate risk, assess alternative approaches, and engage with other government and private sector cyber analysis capabilities to quickly share actionable information. DOE will establish a robust cyber-physical testing capability at national laboratories to analyze systems and component vulnerabilities, malware threats, and impacts of zero-day threats on energy infrastructure; and to support initiatives to harden the supply chain. This will be accomplished by developing requirements and engaging the National Laboratories and private sector."[34]

The 2018 cybersecurity plan also emphasizes the importance of researching, developing, and demonstrating tools and technologies to help prevent a cyber incident. Specific to SCRM, these tools should aim to "decrease the

32 "Energy Department Releases New Guidance for Strengthening Cybersecurity of the Grid's Supply Chain," *Department of Energy*, April 28, 2014, https://www.energy.gov/articles/energy-department-releases-new-guidance-strengthening-cybersecurity-grid-s-supply-chain.

33 "Multiyear Plan for Energy Sector Cybersecurity," *Department of Energy*, March 2018, p. 6.

34 Ibid., p. 25.

risk posed by malicious functionality that could be inserted as components and systems traverse the supply chain."[35] DOE and its partners are already making progress towards this end. The plan notes that "DOE research partnerships are advancing tools and technologies that help identify undesired, potentially malicious, functionality that may have been inserted in hardware, firmware or software of EDS [energy delivery system] components as they traverse the supply chain; that offer guidance on procurement language that purchasers and suppliers of EDS can use as a starting point to discuss needed cybersecurity measures during the EDS process; and that help ensure the integrity of patches and upgrades."[36]

The DOE strategy also calls for "secure code development and software quality assurance (1.2 and 1.3): Secure and safe coding practices can be implemented on new products, but high cost, conflicts with legacy products, and lack of demand remain key barriers. Significant work is needed in awareness and workforce training. Supply chain risk remains a key issue."[37]

In addition, DOE's response to Executive Order No. 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," issued in May 2017, provides encouraging—although not yet tangible—progress. A DOE report acknowledges the severity of supply chain threats to grid components and urges the department to "develop a national laboratory testing program for examining grid components to assess cybersecurity supply chain posture and examine cyber malware impacts to components in a simulated environment."[38] It is currently unclear how much progress, if any, is underway since DOE recommended the initiative in August 2017.

The department is also working with its national laboratories to conduct its own product testing. The Idaho National Laboratory's (INL) Critical Infrastructure Test Range, which includes "test beds" for the electric grid and other cyber components, "allows for scalable physical and cyber performance testing to be conducted on industry-scale infrastructure systems."[39] DOE is also working with other national laboratories for a variety of cybersecurity-

35 Ibid., p. 34.

36 Ibid.

37 Ibid., p. 45.

38 "Section 2(e): Assessment of Electricity Disruption Incident Response Capabilities," *Department of Energy,* August 9, 2017, p. 29.

39 "Securing the Electrical Grid from Cyber and Physical Threats," *Idaho National Laboratory*, https://www.inl.gov/research-programs/grid-resilience/.

related energy sector projects through the National SCADA Test Bed.[40] In addition, DOE is partnering with a handful of national laboratories (with INL as the lead laboratory), other government stakeholders, and industry on the Cyber Testing for Resilience of Industrial Control Systems (CyTRICS) program, which is currently in the pilot stage. Through CyTRICS, DOE intends to test critical components and leverage the test data to identify systemic and supply chain risks.

2. Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC)

FERC is laying the foundations for private sector SCRM requirements in the electricity subsector. In July 2016, FERC directed NERC to develop SCRM reliability standards.[41] Specifically, FERC charged NERC with developing standards that would require entities to develop an SCRM plan focused on four objectives: "(1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls."[42] While they have not yet been subject to enforcement, FERC approved NERC Standards CIP-013-1 (Cyber Security—Supply Chain Risk Management), CIP-005-6 (Cyber Security—Electronic Security Perimeter(s)) and CIP-010-3 (Cyber Security—Configuration Change Management and Vulnerability Assessments) in January 2018.[43] Collectively, FERC believes they address the objectives stated above. CIP-013-1, for example, intends to "mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems."[44]

NERC's supply chain reliability standards are extremely valuable for meeting the supply chain risks in the electricity subsector. Moreover, as

40 "National SCADA Test Bed," *Department of Energy*, https://www.energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity/national-scada-test-bed.

41 "FERC Directs Development of Standards for Supply Chain Cyber Controls," *Federal Energy Regulatory Commission*, July 21, 2016, https://www.ferc.gov/media/news-releases/2016/2016-3/07-21-16-E-8.asp#.WQC2DGnysuU.

42 "Supply Chain Risk Management Reliability Standards (Docket No. RM17-13-000)," *Federal Energy Regulatory Commission,* 162 FERC ¶ 61,044, January 18, 2018, p. 5.

43 Ibid., p. 1.

44 North American Electric Reliability Corporation, "CIP-013-1—Cyber Security—Supply Chain Risk Management," July 2017, p. 3, https://bit.ly/2A1rWyE.

with existing power company initiatives to build resilience against cyber and electromagnetic threats, many companies go above and beyond the requirements of reliability standards and *voluntarily* take additional resilience measures. The same approach makes sense for supply chain security.

While the new standards provide an important baseline for strengthening the electricity subsector's supply chains, they also entail some limitations. For example, due to FERC and NERC's jurisdiction under Section 215 of the Federal Power Act, only certain power industry entities are required to comply with these standards. FERC notes specifically that this does not include "non-jurisdictional suppliers, vendors or other entities that provide products or services to responsible entities."[45] Even among those under FERC and NERC jurisdiction, the standards (with one minor exception) do not apply to Electronic Access Control and Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Protected Cyber Assets (PCAs), or entities considered "low impact." FERC notes that "there remains a significant cyber security risk associated with the supply chain for BES Cyber Systems" as a result.[46]

3. Electricity Subsector Coordinating Council (ESCC)

The ESCC is a critical link between the subsector's government and industry partners. The body and its leadership play an important role in spurring resilience initiatives and contribute significantly to overall grid security. Among those initiatives, the ESCC is working on supply chain security. Specifically, the ESCC is working with the government to convene public and private sector stakeholders, as well as security and technology vendors, "to identify and share best practices to address threats to the supply chain."[47] The ESCC and DOE are also working toward a data-based program to identify systemic supply chain risks and vulnerabilities.

4. Nuclear Regulatory Commission (NRC)

Nuclear energy entities, not subject to FERC/NERC regulation, have their own cybersecurity guidelines. In particular, the NRC's "Protection

45 Federal Energy Regulatory Commission, "Supply Chain Risk Management Reliability Standards (Docket No. RM17-13-000)," 162 FERC ¶ 61,044, January 18, 2018, p. 7.

46 Ibid., p. 3 and 8.

47 "ESCC," *Electricity Subsector Coordinating Council*, January 2018, http://www.electricitysubsector.org/ESCCInitiatives.pdf?v=1.8.

of digital computer and communication systems and networks" lays out cybersecurity requirements for complying entities.[48] Those requirements broadly require entities to ensure the protection of their systems, and do not entail specific SCRM provisions. However, (d)(3) requires entities to "ensure that modifications to assets . . . are evaluated before implementation," which could address vulnerabilities introduced by software and hardware updates. The NRC's regulatory guidance from 2010 does explicitly note the need for SCRM among their operational and management security controls. NRC recommends that facilities protect against supply chain threats and vulnerabilities by establishing trusted distribution paths, validating vendors, and requiring that acquired products are tamper-proof (or have tamper-evident seals).[49] NRC plans to review its cybersecurity regulations in 2019 and update as necessary.[50]

Multi-Sector Initiatives

1. Department of Homeland Security (DHS)

DHS is augmenting its SCRM efforts. DHS established its Cyber Supply Chain Risk Management (C-SCRM) program in January 2018 to serve as the "lead organization and central coordination point for whole-of-government C-SCRM."[51] The initiative has an ambitious vision of enabling "a national and global ICT market and operational environment where the existence of intentionally and negligently misconfigured, poorly manufactured, and counterfeit hardware, components, and software is readily identified, actionable through interdiction or mitigation, and rare."[52] DHS also outlined the program's major activities to:

- establish a supply chain risk assessment capability to serve stakeholders

48 US Nuclear Regulatory Commission, "§ 73.54 Protection of digital computer and communication systems and networks," 2009, https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html.

49 US Nuclear Regulatory Commission, "Regulatory Guide 5.71: Cyber Security Programs for Nuclear Facilities," January 2010, pp. C-29–C-30, https://www.nrc.gov/docs/ML0903/ML090340159.pdf.

50 Sean Lyngaas, "Nuclear Power Plants Have a 'Blind Spot' for Hackers. Here's How to Fix That," *Motherboard*, April 27, 2018, https://motherboard.vice.com/en_us/article/mbxy33/cyberattacks-nuclear-supply-chain.

51 Department of Homeland Security, "Cyber Supply Chain Risk Management: Becoming a Smarter Consumer of ICT in a Connected World," June 2018, p. 15.

52 Ibid.

- establish a communications, notification, and information-sharing capability among stakeholders
- establish qualified bidder and manufacturer lists through implementing a robust process for validating and approving the security practices of companies and the security characteristics of ICT products and services
- provide stakeholders with assistance in developing and implementing supply chain risk management capabilities.[53]

The C-SCRM imitative, which includes General Services Administration (GSA), the Department of Defense (DOD), the intelligence community, and private sector stakeholders, is intended to help inform government procurement decisions.[54] According to a DHS official, the initiative will "provide actionable information about supply chain risks and mitigations to users, buyers, manufacturers and sellers of tech products. It will also identify risks to federal networks and other national or global stakeholders."[55] Assistant Secretary for the Office of Cybersecurity and Communications at the National Protection and Programs Directorate (NPPD) Jeanette Manfra further noted that the C-SCRM initiative will "identify and mitigate supply chain threats and vulnerabilities" to high-value assets.[56]

The initiative builds on valuable, existing DHS tools for addressing supply chain risks. The Continuous Diagnostics and Mitigation (CDM) program, for example, contains an acquisition strategy to mitigate supply chain-based cyber threats. This strategy includes the Approved Products List (APL), an "authoritative product catalog that has been approved to meet CDM technical capability requirements."[57] Through the CDM/APL, DHS also has a specific SCRM plan, the objective of which is to "provide information to Agencies

53 Ibid., p. 16.

54 Jory Heckman, "DHS, Lawmakers Doubling down on Supply Chain Risk Management," *Federal News Radio,* February 15, 2018, https://federalnewsradio.com/cybersecurity/2018/02/dhs-lawmakers-doubling-down-on-supply-chain-risk-management/.

55 Lauren C. Williams, "DHS Developing Supply Chain Security Initiative," *FCW,* February 14, 2018, https://fcw.com/articles/2018/02/14/dhs-supply-chain-security.aspx.

56 *US House of Representatives Committee on Oversight and Government Reform Subcommittee on Information Technology* (2018) (statement of Jeannette Manfra, Assistant Secretary for Cybersecurity and Communications, NPPD), DHS, p. 8.

57 "Continuous Diagnostics and Mitigation (CDM)," *Department of Homeland Security*, last updated February 22, 2018, https://www.dhs.gov/cdm.

and ordering activities about how the offeror identifies, assesses, and mitigates supply chain risks in order to facilitate better informed decision-making by Agencies and ordering activities."[58]

2. National Institute of Standards and Technology (NIST)

NIST is a leading source of SCRM guidance. NIST's Computer Security Resource Center (CSRC) has a major Cyber Supply Chain Risk Management program. Notably, the CSRC recognizes the supply chain threats to IT and OT networks.[59] NIST's 2015 SCRM publication provides comprehensive guidance on managing cyber supply chain risks. The guidelines provide a framework for federal departments and agencies which "can be modified or augmented with organization-specific requirements from policies, guidelines, and other documents."[60] The document presents a set of processes and measures for evaluating and managing supply chain risk and provides a template for developing SCRM plans. NIST also provides a set of SCRM best practices applicable to all infrastructure sectors.[61] Moreover, NIST's updates to their "Framework for Improving Critical Infrastructure Cybersecurity" (Cybersecurity Framework) in 2017 included "new details on managing cyber supply chain risks,"[62] while the April 2018 update includes further revisions on "managing cybersecurity within the supply chain."[63]

In addition to these initiatives and guidelines, NIST convenes leaders from government, the private sector, and academia to address supply chain

58 Government Services Agency, "Continuous Diagnostics and Mitigation (CDM) Approved Products List (APL) Supply Chain Risk Management (SCRM) Plan," August 2017, p. 1.

59 "Cyber Supply Chain Risk Management," *National Institute of Standards and Technology.*

60 National Institute of Standards and Technology "Supply Chain Risk Management Practices for Federal Information Systems and Organizations (SP 800-161)," April 2015, p. 2.

61 National Institute of Standards and Technology, "Utility Sector Best Practices for Cyber Security Supply Chain Risk Management," October 2015, https://www.nist.gov/sites/default/files/documents/itl/csd/USRP_NIST-Utility_100115.pdf.

62 "NIST Releases Update to Cybersecurity Framework," *National Institute of Standards and Technology*, January 10, 2017, https://www.nist.gov/news-events/news/2017/01/nist-releases-update-cybersecurity-framework.

63 "NIST Releases Version 1.1 of its Popular Cybersecurity Framework," *National Institute of Standards and Technology*, April 16, 2018, https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework.

risks. The Software and Supply Chain Assurance Forum, co-led by DHS, GSA, and DOD, allows participants to "share their knowledge and expertise regarding software and supply chain risks, effective practices and mitigation strategies, tools and technologies, and any gaps related to the people, processes, or technologies involved."[64]

This sharing and coordination function is helpful; however, it falls drastically short of need. It would be incredibly expensive and altogether impractical to assume that individual participants in this process would develop their own product certification mechanisms, fully share their conclusions with their colleagues, and create the unified "demand pull" needed to grow the supply of certified products.

3. Office of Management and Budget (OMB)

The OMB provides a key source of federal government cybersecurity policy. Indeed, the Federal Information Security Modernization Act (FISMA) requires the OMB to oversee agency information security policies and practices. The "OMB Circular A-130: Managing Information as a Strategic Resource," issued in 2016, establishes "general policy for the planning, budgeting, governance, acquisition, and management of Federal information, personnel, equipment, funds, IT resources and supporting infrastructure and services" for the executive branch of the federal government.[65] A-130 contains the primary guidance to such agencies for implementation of FISMA and includes some guidance for federal SCRM. Particularly, the document states that agencies shall:

- "consider . . . supply chain security issues for all resource planning and management activities throughout the system development life cycle so that risks are appropriately managed;"
- "analyze risks (including supply chain risks) associated with potential contractors and the products and services they provide."[66]

64 "Software and Supply Chain Assurance Forum," *National Institute of Standards and Technology*, last updated March 29, 2018, https://csrc.nist.gov/Projects/Supply-Chain-Risk-Management/SSCA.

65 Office of Management and Budget, "Circular No. A-130: Managing Information as a Strategic Resource," July 2017, p. 6, https://bit.ly/2rAjz7Q.

66 Ibid., p. 6 and 11.

An Appendix to A-130 which "establishes minimum requirements for federal information security programs" also requires agencies to:

- "implement supply chain risk management principles to protect against the insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software, as well as poor manufacturing and development practices throughout the system development life cycle;"
- "develop supply chain risk management plans as described in NIST SP 800-161 to ensure the integrity, security, resilience, and quality of information systems."[67]

If implemented and stringently verified, the A-130 could contribute to the security of executive branch supply chains. However, the policy provides little in terms of specific requirements, other than deferring to the NIST guidance examined above. It also requires each agency to create their own SCRM program, which—as noted throughout—is not economically feasible to achieve at the required level of comprehension.

Moreover, while the policy applies to the majority of Sector-specific agencies (SSA) (except, critically, the Environmental Protection Agency as SSA for the water and wastewater sector), it is limited to only a subset of government agencies and does not apply to industry or other stakeholders.

4. General Services Administration (GSA)

GSA plays a key role in federal government acquisition and, accordingly, in securing federal IT supply chains. Specifically, GSA is "establishing a comprehensive SCRM capability that will ensure government agencies procure IT hardware and software from original equipment manufacturers, including authorized resellers or other trusted sources."[68] They are also establishing a Vendor Risk Assessment Program (VRAP) to "evaluate known or potential risks related to suppliers of products and services."[69]

67 Ibid., p. 40 and 42.

68 Shon Lyublanovits, "Reducing Cybersecurity Risks in Supply Chain Risk Management," *General Services Administration*, September 18, 2017, https://gsablogs.gsa.gov/technology/2017/09/18/reducing-cybersecurity-risks-in-supply-chain-risk-management/.

69 Ibid.

5. Office of the Director of National Intelligence (ODNI) and the National Counterintelligence and Security Center (NCSC)

ODNI has produced SCRM policy for the intelligence community. Intelligence Community Directive 731, in particular, is the policy "to protect the supply chain as it relates to the lifecycle of mission-critical products, materials, and services used by the IC through the identification, assessment, and mitigation of threats."[70] It is supplemented by specific directives on determining the mission criticality of components, details on conducting threat assessments, and improving information sharing.

In addition to the directives, ODNI's NCSC also has highlighted SCRM threats. A 2013 white paper and 2017 backgrounder provide succinct yet valuable introductions to cyber supply chain threats and risk management.[71] In cooperation with DHS, NCSC also launched an industry partnership that is contributing to SCRM efforts. The Public-Private Analytic Exchange Program (AEP) first identified cyber SCRM risks as a major focus for the electricity subsector in a 2016 white paper. The report offers key SCRM findings and recommendations for both industry and government.[72] A more detailed report from 2017 builds on that white paper to provide more comprehensive recommendations, specifically regarding OT threats. AEP produced the report to "highlight potential security risks to the SCADA supply chain in the current nascent stage to prevent an expensive, future retrofit of an established industry."[73]

While the report is still largely an information product with recommendations rather than a detailed basis for concrete action, it nevertheless provides extremely valuable context and highlights the NCSC—and the AEP in particular—as a potentially valuable partner for CPIC. This is especially true since implementing the recommendations of the AEP report of having companies build their own certification mechanisms and create the market forces necessary to grow the supply of certified hardware and software is untenable.

---

70 Office of the Director of National Intelligence, "Intelligence Community Directive 731 – Supply Chain Risk Management," December 2013, p. 1.

71 NCSC, *Supply Chain Risk Management: Framework for Assessing Risk*.

72 Public-Private Analytic Exchange Program, "Identifying and Mitigating Supply Chain Risks."

73 Ibid., p. iii.

6. Department of Defense (DOD)

DOD also has an SCRM policy to achieve "trusted" systems and networks. Last updated in July 2017, DOD Instruction 5200.44 "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks" establishes policies to minimize the risks related to "vulnerabilities in system design or sabotage or subversion of a system's mission critical functions or critical components . . . by foreign intelligence, terrorists, or other hostile elements."[74] The instruction emphasizes the importance of managing supply chain risks through the entirety of a product's lifecycle. This policy is specific to DOD's mission-critical functions, although similar principles and approaches can be applied to the CPIC's efforts and general approach.

7. White House

The White House emphasizes the importance of securing global supply chains in two separate initiatives. To manage supply chain risks the "National Strategy for Global Supply Chain Security," issued in January 2012, calls for a greater understanding of supply chain threats that stem from "exploitation of the system by those seeking to introduce harmful products or materials."[75] The White House's Comprehensive National Cybersecurity Initiative also highlights supply chain threats. Initiative 11 is to "develop a multi-pronged approach for global supply chain risk management," in which managing risks will involve "the development and employment of tools and resources to technically and operationally mitigate risk across the lifecycle of products (from design through retirement) . . . and partnership with industry to develop and adopt supply chain and risk management standards and best practices."[76]

Private Sector Initiatives

One private sector initiative is particularly promising and deserving of consideration: the Charter of Trust Initiative. Siemens recently joined with the Munich Security Conference and other governmental and business partners (including IBM and AES) to launch this initiative. The charter is intended

74 Department of Defense, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)," Instruction No. 5200.44, last updated July 27, 2017, p. 1.

75 White House, "National Strategy for Global Supply Chain Security," January 2012, p. 4.

76 White House, "The Comprehensive National Cybersecurity Initiative," March 2010, https://obamawhitehouse.archives.gov/node/233086.

to "develop and implement rules for ensuring cybersecurity throughout the networked environment."[77]

Principle 7 of the charter offers a possible focus for dialog with Siemens and its charter partners. This principle states that "companies—and if necessary—governments establish mandatory independent third-party certifications (based on future-proof definitions, where life and limb is at risk in particular) for critical infrastructure as well as critical IoT solutions."[78] This provides an opportunity for CPIC to partner with Charter of Trust participants on collaborative SCRM solutions that leverage each initiative's strengths and resources.

Product Certification

Product certification-focused organizations and initiatives exist, largely in the private sector, to assess potential risks to specific products, processes, and systems. A significant number of these organizations and certification schemes exist worldwide, although only a few are surveyed here. Many of these certification bodies include considerations for cybersecurity, although few certify for electromagnetic thresholds.

1. Underwriters Laboratories (UL)

UL provides a wide array of certification services, ranging from specific products, facilities, processes, or systems to industry-wide standards and requirements.[79] As an industry leader in the United States, working with manufacturers, industry experts, other testing labs, and governments, UL testing standards are often considered the "de facto standards of the US government."[80] UL can also serve as an independent third party to certify

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

78 "Charter of Trust: For a Secure Digital World," *Charter of Trust,* February 2018, https://www.siemens.com/press/pool/de/feature/2018/corporate/2018-02-cybersecurity/charter-of-trust-e.pdf.

79 "Certification," *Underwriters Laboratories,* https://services.ul.com/categories/certification/.

80 Mike Murphy, "Inside the 122-year-old Company that Makes Sure our Electronics Don't Blow up our Homes," *Quartz*, April 5, 2016, https://qz.com/643007/inside-the-122-year-old-company-that-makes-sure-our-electronics-dont-blow-up-our-homes/.

supply chains and related processes.[81] The US Department of Labor's Occupational Safety and Health Administration considers UL as one of its Nationally Recognized Testing Laboratories.[82]

2. International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)

ISO and IEC are two separate entities that cooperate to create industry and product standards and certification. Specifically, the ISO/IEC Joint Technical Committee (JTC) 1 focuses on standards development for IT.[83] ISO/IEC standard 27036, of which there are four parts, provides guidelines "to assist organizations in securing their information and information systems within the context of supplier relationships."[84] Outside of this joint work, the IEC also develops electromagnetic standards, including those for "complex products or those that operate in a special environment."[85]

The IEC's 62443 series of standards offer an especially useful model for further analysis. These standards address the need to design cybersecurity robustness and resilience into industrial automation control systems (IACS). In particular, the 62443-4-1 standard describes the derived requirements that are applicable to the development of control system products.[86] The ISO/IEC standards can help inform the criteria for future certification schemes, although further outreach will be necessary to determine the extent to which (and how) ISO/IEC provides continuing testing and verification of products and vendors.

---

81 "Supply Chain Certification," *Underwriters Laboratories*, https://services.ul.com/service/supply-chain-certification/.

82 "Current List of NTRLs," *Occupational Safety and Health Administration*, https://www.osha.gov/dts/otpca/nrtl/nrtllist.html.

83 "ISO/IEC JTC 1 — Information Technology," *International Organization for Standardization*, https://www.iso.org/isoiec-jtc-1.html.

84 "ISO/IEC 27036-1:2014," *International Organization for Standardization*, April 2014, https://www.iso.org/standard/59648.html.

85 "EMC Product Standards," *International Electrotechnical Commission*, 2018, http://www.iec.ch/emc/emc_prod/.

86 "Overview – The 62443 Series of Standards," *ISA, 2015*, https://fr.scribd.com/document/358894928/ISA-62443-Series-Overview.

3. The SAFETY Act (DHS)

DHS has a product certification scheme for anti-terrorism technologies. In the wake of the 9/11 attacks, the private sector was "extremely reluctant to deploy security technologies and services in civilian settings due to the enormous liability risks involved."[87] These companies would be liable if their product did not stop or mitigate the attack it was designed to prevent. In response, Congress enacted the Support Anti-Terrorism by Fostering Effective Technologies Act (SAFETY Act) in 2002 "to ensure that the threat of liability does not deter potential manufacturers or sellers of effective anti-terrorism technologies from developing and commercializing technologies that could save lives."[88] The SAFETY Act contains a mechanism to certify a broad range of products, services, and technologies as Qualified Anti-Terrorism Technologies (QATT), placing them on the Approved SAFETY Act Product List for Homeland Security.[89] DHS grants liability limitations for the sellers and users of such QATTs.[90] Among the products currently approved for SAFETY Act liability protections are cybersecurity technologies.[91]

4. International Cybersecurity Certification Programs

A number of certification mechanisms and bodies exist to ensure the cybersecurity of products. Indeed, tiered security certification for commercial IT products has existed for over thirty years.[92] The criteria that inform these certification schemes have been enshrined in standards, such as the Common Criteria (CC). CC has also established an extensive certification arrangement, which includes a product certification scheme. The objectives of this arrangement include ensuring the high-quality evaluation of IT products, improving the availability of certifiably secure products, eliminating the burden of duplicate evaluations, and continuously improving "the efficiency

87 Department of Homeland Security, "Research and Development Partnerships – SAFETY Act for Liability Protection," January 14, 2014, https://bit.ly/2JPIolm.

88 Department of Homeland Security, "The Office of SAFETY Act Implementation," https://www.dhs.gov/science-and-technology/safety-act.

89 Department of Homeland Security, "Research and Development Partnerships – SAFETY Act for Liability Protection," January 14, 2014, https://bit.ly/2JPIolm.

90 Ibid.

91 Ibid.

92 Steven B. Lipner, *SAFECode Perspective on Cybersecurity Certification*, January 2018, p. 1, https://safecode.org/wp-content/uploads/2018/02/SAFECode_Perspective_on_Cybersecurity_Certification.pdf.

and cost-effectiveness of the evaluation and certification/validation process."[93] CC has certified 2,351 products as of June 5, 2018, which include access control devices and systems, operating systems, detection devices and systems, and boundary protection devices and systems.[94]

As with many cybersecurity-focused (rather than specifically infrastructure-focused) initiatives, one potential flaw lies in the CC's focus on IT rather than OT. In addition, its membership does not include any participation from China, Russia, or any other near-peer cyber adversaries.[95] The membership structure, however, does include a management committee with senior representatives from each signatory country "to implement the Arrangement and to provide guidance to the respective national schemes conducting evaluation and validation activities."[96]

A range of other public and private sector cybersecurity certification programs exist. As mentioned above, some SCRM initiatives may be inherently compromised by the membership of their founding organization. While the Open Group boast an international membership of over 500, with an extremely large US contingent, this organization extends to the point of including potential adversaries. SAFECode's membership is much smaller, but nevertheless includes the same potential adversary.

a. SAFECode

The SAFECode program, a software assurance-focused, EU-based organization, has a similar vision to CPIC. SAFECode is looking to help users "identify products and online services that provide effective security and can incentivize suppliers to invest in effective security—and help to ensure that they are rewarded for that investment."[97] Notably, SAFECode is helping the small and mid-sized organizations that are struggling to keep up with major organizations worldwide, which have funded their own SCRM programs.[98]

---

93 "About the Common Criteria," *Common Criteria*, https://www.commoncriteriaportal.org/ccra/index.cfm.

94 "Certified Products," *Common Criteria*, https://www.commoncriteriaportal.org/products/.

95 "Members of the CCRA," *Common Criteria*, https://www.commoncriteriaportal.org/ccra/members/.

96 "About the Common Criteria," *Common Criteria*.

97 Lipner, *SAFECode Perspective on Cybersecurity Certification*, p. 2.

98 Ibid., p. 3.

CPIC addresses this challenge by centralizing the resources required to secure supply chains and by creating a strong, consistent "demand signal" for the production of secure products.

SAFECode's backgrounder on cybersecurity certification provides a number of important perspectives. Critically, SAFECode emphasizes the importance of certifying a product while it is being developed—rather than after it is released for sale—to ensure that companies do not rely on a product with potential vulnerabilities while certification is pending.[99] Moreover, in highlighting the value of a tiered certification system, SAFECode notes that "schemes that provide varying levels of certification incentivize developers to seek the highest levels of certification."[100] In addition, SAFECode underscores the inherent international footprint of today's supply chains, urging "broad mutual recognition in order to provide maximum benefit to users and developers worldwide."[101]

SAFECode has limitations for infrastructure SCRM as its sole focus is on IT (rather than OT) products. SAFECode also appears to place the onus for compliance, testing, and verification on the organizations themselves, which leads to a drastic duplication of resources and other inefficiencies. SAFECode's "Fundamental Practices for Secure Software Development" can nevertheless provide an additional source of insights for future certification programs.[102]

b. O-TTPS Certification Program

The Open Group O-TTPS program includes guidelines, recommendations, requirements, and best practices aimed at "enhancing the integrity of [commercial off-the-shelf and communication technology] products and the security of their global supply chains."[103] The Open Group certifies

99 Ibid., p. 2.

100 Ibid.

101 Ibid.

102 SAFECode, "Fundamental Practices for Secure Software Development: Essential Elements of a Secure Development Lifecycle Program (Third Edition)," March 2018, https://safecode.org/wp- content/ uploads/2018/03/SAFECode_Fundamental_Practices_for_Secure_Software_Development_March_2018.pdf.

103 "The Open Trusted Technology Provider Standard (O-TTPS) Certification Program," *The Open Group*, http://www.opengroup.org/certifications/o-ttps.

organizations that they deem to comply with the program requirements as "Open Trusted Technology Providers."[104]

O-TTPS policy and guidance documents can also provide important foundational material for future initiatives. The 2017 certification policy document, for example, includes detailed workflow diagrams for third-party certification, with additional detail for each step of the process.[105] The document also includes specific policies for conformance requirements, maintaining certification, re-certification, and an appeal process for certification decisions, among others.

The CPIC Initiative

The Cyber Product International Certification (CPIC) initiative proposed by the EIS Council will help meet many of the challenges outlined above. At present, infrastructure owners and operators lack a compressive, stakeholder-driven process to certify that crucial hardware and software products are even minimally scrubbed of malware and other means of adversary exploitation. Establishing such a certification process would make an enormous contribution to cyber resilience, especially if government agencies can provide threat information and other forms of support for the initiative. CPIC could also meaningfully contribute to infrastructure resilience by including measures to certify products against intentional electromagnetic interference (IEMI). Key issues for consideration in developing the CPIC initiative are:

1. Leveraging existing company plans and capabilities for SCRM

Many private sector entities already have procurement guidelines that constitute potential best practices. While the degree to which these best practices are implemented may vary, they nevertheless can form an important foundation for developing the CPIC initiative. Moreover, just as important, these companies have already developed a business case to strengthen their supply chain security and—in many cases—pay more for products that are more secure. Capturing these best practices would be extremely valuable.

104 Ibid.

105 See The Open Group, "Open Trusted Technology Provider Standard (O-TTPS) Certification Policy (Version 1.1)," January 2017, pp. 14–18, https://ottps-cert.opengroup.org/sites/ottps-cert.opengroup.org/files/doc/O-TTPS_Certification_Policy.pdf.

2. Centralized coordination

Internal SCRM models often require each organization to develop and implement their own certification processes for the products and suppliers they use. The cost of doing so—especially when considering the resources required for implementation and verification—can be significant for each individual organization. With CPIC, however, these costs would be proportionally split among participants, drastically reducing the current duplication of effort and resources, and incentivizing and enabling far more comprehensive certification and validation processes than those considered practical today.

3. Guarding against "minimalist" standards

Although they are helpful, standards that constitute the minimum required SCRM measures are not sufficient to ensure the security of global supply chains. Rep. Langevin has urged that "rather than having just a compliance-based mindset that encourages doing the bare minimum," we should "properly incentivize organizations to take a risk-based approach to cybersecurity," including SCRM.[106] Similarly, the AEP urges government and industry to "incentivize business and economic development in response to supply chain security shortfalls," moving away from a reactive cybersecurity model to a more proactive one that "acknowledges and mitigates inherent and potentially introduced supply chain risks."[107]

To address growing SCRM threats, CPIC should employ a non-regulatory approach, focused on certification of best practices rather than minimalist, broad-brush standards. To be sure, the regulatory measures examined in this brief all provide an essential foundation for CPIC's envisioned capabilities and structure. However, CPIC should not replace these standards as a means of securing supply chains. Rather, the initiative is meant to provide companies with trusted, best-in-class options for ensuring supply chain integrity.

Avoiding a standards-based model will also help CPIC refrain from calcifying into a regulatory structure that defeats its best practice intent. Regulatory requirements inevitably move far slower than the threats they are designed to address and also rarely represent best practices. While the CPIC

106 Lauren C. Williams, "DHS Developing Supply Chain Security Initiative," *FCW*, February 14, 2018, https://fcw.com/articles/2018/02/14/dhs-supply-chain-security.aspx.

107 Public-Private Analytic Exchange Program, "Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector," p. 2.

initiative should be compatible with regulatory schemes and requirements, it will be most effective if it is not constrained by them. Ideally, all CPIC certification processes will also have built-in sunset provisions that require periodic reevaluation and updates to meet the newest assessments of evolving threats.

4. Internationalizing CPIC from the start

The vast majority of contemporary supply chains have an international footprint. Yet, most regulatory standards and guidelines are country-specific. For example, with the exception of the Charter of Trust and cybersecurity-specific certification programs, all of the initiatives and models examined in this report are exclusively focused on the United States (though the NERC standards apply to registered bulk power system entities in Canada and Mexico). However, the United Kingdom, Israel, and the other nations also have cutting-edge SCRM initiatives underway that would be valuable to incorporate. Internationalizing the CPIC effort can help create and expand the necessary customer and product user base as well. Supply chain exploitation efforts by Russia, China, and other nations are multi-sector and global in nature. The CPIC initiative should be structured accordingly.

5. Tiered system

The CPIC Commission should consider developing a tiered product certification system. Such a layered structure could include: (1) a Basic Level, above current regulatory standards but not quite "best-in-class" requirements; and (2) the Prime Certification that sets the standard for best-in-class requirements. In fact, by leveraging the market incentives that would be created by many thousands of secure product customers across multiple sectors, this "Prime Certification" level might even become a "better than best-in-class" certification capability.

6. Role of government

While CPIC will be industry-driven, government participation can ensure that the CPIC initiative: (1) can benefit from senior leaders' expertise; (2) will be maximally compatible with participating government stakeholders' own needs; (3) has inherent credibility with those stakeholders; (4) can be integrated seamlessly with existing government initiatives; and (5) incorporates

government priorities to reduce costs. Incorporating government officials from multiple participating countries will provide added benefit by integrating a range of approaches and perspectives but could also create challenges given the disparate levels of influence each government may have on domestic private sector companies.

Conclusion

Reports by the US intelligence community, DHS, DOE, and other agencies highlight the degree to which supply chain exploitation efforts are metastasizing and becoming ever more difficult to detect.

In the electricity subsector and beyond, industry and government are partnering on aggressive, much-needed efforts to manage supply chain risks. CPIC should avoid "re-inventing the wheel" and replicating work that is already underway. Instead, the initiative should be structured to support and fill gaps between these ongoing programs, in ways that are uniquely possible through the CPIC structure and provide the greatest benefits for infrastructure resilience. This report provided a brief overview of ongoing efforts to facilitate future discussions and identify areas where CPIC can make the most meaningful contributions.

Infrastructure owners and operators are also increasingly focused on buying products that are malware-free. By establishing a private sector-founded and sanctioned product certification process developed in coordination with government agencies, and by purchasing products that meet its standards, owners and operators can help bolster the emerging standards and market forces essential to improve SCRM.

Nuclear Crisis Management and Deterrence: Stalked by Cyberwar?

Stephen J. Cimbala

Cyberwar, preceding or during nuclear crises, can marginally or even fatally strain the requirements of nuclear deterrence stability and is capable of disrupting the communications between governments in times of crisis or confusing their assessments of ongoing events. This discussion considers the requirements for successful nuclear crisis management, the possible vulnerabilities induced by cyberwar, and the scenarios in which opportunistic failure is possible.

Keywords: Cyberwar, information warfare, deterrence, crisis stability, nuclear war, management, command-control, networks, communications, escalation control

Introduction

The information age and its military-technical applications obviously will cause some changes in the character and attributes of nuclear deterrence. Exactly how cyberwar and nuclear deterrence might coexist or compete as paradigms for policy consideration is less apparent. Although cyber operations differ from kinetic operations, the various components of information warfare "should now increasingly be considered elements of a larger whole rather than

Stephen J. Cimbala is Distinguished Professor of Political Science at Penn State Brandywine. The author gratefully acknowledges Paul Davis, Andrew Futter, Lawrence Korb, and Timothy Thomas for insights into the topic of this study. They bear no responsibility for its content.

separate specialties that individually support kinetic military operations."[1] For example, Pavel K. Baev suggests that a new blend of corruption, intelligence operations, cyberattacks, and propaganda offensives is now the "trademark" of Russian foreign policy and requires a new kind of Western deterrence.[2]

If the ultimate weapons of mass destruction—nuclear weapons—and the supreme weapons of soft power—information warfare—are commingled during a crisis, the product of the two may be an entirely unforeseen and unwelcomed hybrid. Crises by definition are exceptional events. No cold war crisis between states armed with both twenty-first century information weapons and nuclear weapons has yet occurred. In addition, the nuclear-cyber relationship has special significance for the United States and Russia: The two powers hold more than 90 percent of the world's nuclear weapons, and both have advanced offensive and defensive cyberwar capabilities.[3] The

1 Martin C. Libicki, "The Convergence of Information Warfare," *Strategic Studies Quarterly* no. 1 (Spring 2017), p. 50 and see also pp. 49–65. In this study I use the terms "information warfare" and "cyberwar" interchangeably and generically, although some cyber grammarians might insist that "cyberwar" be restricted to digital attacks on information systems and networks *per se*, and information warfare to broader kinds of influence operations, possibly including digital and/or other methods. A sensible approach to this matter is used in P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014), pp. 67–72 and passim, and in John Arquilla, *Worst Enemy: The Reluctant Transformation of the American Military* (Chicago: Ivan R. Dee, 2008), ch. 6–7, in addition to sources in later notes.

2 Pavel K. Baev, "Corruption Spoils Every Attempt to Cooperate With Russia," *Eurasia Daily Monitor*, July 17, 2017, https://jamestown.org/analyst/pavel-k-baev, accessed August 7, 2017.

3 For a discussion of Russian cyber capabilities and doctrines, see Timothy L. Thomas, *Russia: Military Strategy—Impacting 21st Century Reform and Geopolitics* (Ft. Leavenworth, Kansas: Foreign Military Studies Office, 2015), pp. 253–299; for pertinent insights on the topic of cyber war and nuclear war, see Erik Gartzke and Jon R. Lindsay, "Thermonuclear Cyberwar*, Journal of Cybersecurity* (2017), pp. 1–12, https://doi:10.1093/cybsec/tyw017; Andrew Futter, "The Double-Edged Word: US Nuclear Command and Control Modernization," *Bulletin of the Atomic Scientists*, June 29, 2016, http://thebulletin.org/double-edged-sword-us-nuclear-command-and-control-modernization.html; Andrew Futter, "Cyber Threats and Nuclear Weapons: New Questions for Command and Control, Security and Strategy," *RUSI Occasional Paper* (July 2016), https://rusi.org/sites/default/files/cyber_threats_and_nuclear_combined.1.pdf; and Andrew Futter, "War Games Redux? Cyberthreats, U.S.-Russian Strategic Stability, and New Challenges for Nuclear Security and Arms Control," *European Security* (December 2015): 163–180.

discussion below proceeds toward that end in several steps. We consider concepts and definitions of crisis management; attributes and requirements for successful crisis management; challenges posed by information operations and cyberwar for nuclear crisis stability; and, finally, some possibly dangerous scenarios in which cyber-spiked nuclear crisis management might be especially problematic.

Crisis Management

Concepts and Definitions

Crisis management, including nuclear crisis management, is both a competitive and cooperative endeavor between military adversaries. By definition, a crisis is a time of great tension and uncertainty.[4] Threats are in the air and the time pressure on policymakers seems intense. Each side has objectives that it wants to attain and values or interests that it deems important to protect. During a crisis state, behaviors are especially interactive and interdependent with those of another state. It would not be too farfetched to refer to this interdependent stream of interstate crisis behaviors as a system, provided the term "system" is not understood as an entity completely separate from the state or individual behaviors that compose it. The system aspect implies reciprocal causation of the crisis behaviors of "A" by "B," and vice-versa.

One aspect of crisis management is the deceptively simple question: What defines a crisis as such? When does the latent capacity of the international order for violence or hostile threat assessment cross over into the terrain of actual crisis behavior? A breakdown of general deterrence in the system raises threat perceptions among various actors, but it does not guarantee that any particular relationship will deteriorate into specific deterrent or

4 For the political and operational requirements of crisis management, see Alexander L. George, "A Provisional Theory of Crisis Management," in *Avoiding War: Problems of Crisis Management*, ed. Alexander L. George (Boulder: Westview Press, 1991), pp. 22–27; for descriptions of offensive and defensive crisis management strategies, see Alexander L. George, "Strategies for Crisis Management," in *Avoiding War*, ed. Alexander L. George, pp. 377–394. See also, Ole R. Holsti, "Crisis Decision Making," in *Behavior, Society and Nuclear War*, ed. Philip E. Tetlock et al. (New York: Oxford University Press, 1989), 1:8–84; and Phil Williams, *Crisis Management* (New York: John Wiley and Sons, 1976). See also Alexander L. George, "The Cuban Missile Crisis: Peaceful Resolution Through Coercive Diplomacy," in *The Limits of Coercive Diplomacy,* ed. Alexander L. George and William E. Simons, 2nd ed.(Boulder: Westview Press, 1994), pp. 111–132.

compellent threats. Patrick Morgan's concept of "immediate" deterrence failure is useful in defining the onset of a crisis: One state identifies specific sources of hostile intent from another, they exchange threats, and they must now determine responses.[5] The passage into a crisis is equivalent to the shift from Hobbes' world of omnipresent potential for violence to the actual movement of troops and exchanges of diplomatic demarches.

All crises are characterized to some extent by a high degree of threat (rapid escalatory momentum, with the meaningful and imminent risk of reaching more intensive hostilities; yet neither party has elected full hostilities and both parties still prioritize a de-escalation), limited time for decision, and a "fog of crisis" reminiscent of Clausewitz's "fog of war" that confuses crisis participants about what is happening. Before modern scholars had even invented the discipline of crisis management, historians had captured the rush-to-judgment character of much crisis decision making among the great powers.[6] The influence of nuclear weapons on crisis decision making is therefore not easy to measure or document because the avoidance of war can be ascribed to many causes. The presence of nuclear forces obviously influences the degree of destruction that could take place should crisis management fail and is therefore often a de-escalatory factor. Short of that catastrophe, scholars are greatly interested in how the presence of nuclear weapons might affect the decision-making process during a crisis. The problem is conceptually elusive as many potentially important causal factors are relevant to a decision about war or peace. History is full of dependent variables in search of competing explanations.

Crisis Management: The Requirements

First, successful crisis management requires communications transparency, although this generalization acknowledges that vague or oblique communication

5 See Patrick M. Morgan, *Deterrence: A Conceptual Analysis* (Beverly Hills: Sage Publications, 1983) and Richard Ned Lebow and Janice Gross Stein, *We All Lost the Cold War* (Princeton: Princeton University Press, 1994), pp. 351–355.

6 For example, see Richard Ned Lebow, *Between Peace and War: The Nature of International Crisis* (Baltimore: Johns Hopkins University Press, 1981); Michael Howard, *Studies in War and Peace* (New York: Viking Press, 1971), pp. 99–109; Gerhard Ritter, *The Schlieffen Plan: Critique of a Myth* (London: Oswald Wolff, 1958); and D. C. B. Lieven, *Russia and the Origins of the First World War* (New York: St. Martin's Press, 1983).

is useful in specific cases, such as the way Iran behaved in the crisis over its nuclear project. Transparency includes clear signaling and undistorted communications. Signaling refers to the requirement that each side must send the other its estimate of the situation. Although it is not necessary for the two sides to have identical or even initially complementary interests, a sufficient number of correctly sent and received signals is prerequisite to effectively transmit goals and objectives from one side to the other. If signals are poorly sent or misunderstood, steps taken by the sender or receiver may cause unintended consequences, including miscalculated escalation. The gravity of the situation may require complete transparency, although there are many examples in which only partial communication sufficed. Moreover, communication is not necessarily verbal; rather, it can be kinetic as in the assembly of forces or military preparations and signals of resolve.

Communications transparency also includes high-fidelity and technically dependable communication between adversaries and within the decision-making structures of each side. Everything that might interfere physically, mechanically, or behaviorally with accurate transmission can distort high-fidelity communication in a crisis. Electromagnetic pulses that disrupt communication circuitry or physical destruction of communication networks are obvious examples of impediments to high-fidelity communication. Cultural differences that prevent accurate understanding between states can confound deterrence as practiced according to one side's theory. As Keith B. Payne notes about the potential for deterrence failure in the post-Cold War period: "Unfortunately, our expectations of opponents' behavior frequently are unmet, not because our opponents necessarily are irrational but because we do not understand them—their individual values, goals, determination, and commitments—in the context of the engagement, and therefore we are surprised when their 'unreasonable' behavior differs from our expectations."[7]

Second, successful crisis management requires that the pressure of time exerted upon policymakers and commanders be minimized so that they do not take unintended, provocative steps toward escalation because they have misperceived that "time is up." Time pressure is one thing, but unintended

7 Keith B. Payne, *Deterrence in the Second Nuclear Age* (Lexington: University Press of Kentucky, 1996), p. 57. See also David Jablonsky, *Strategic Rationality Is Not Enough: Hitler and the Concept of Crazy States* (Carlisle Barracks, PA: US Army War College, Strategic Studies Institute, August 8, 1991), esp. pp. 5–8 and pp. 31–37.

steps are another. Policymakers and military planners are capable of inventing fictive worlds of perception and evaluation in which the "H hour" becomes more than a useful benchmark for decision closure. In the decision pathologies possible in crisis conditions, deadlines may be confused with policy objectives themselves: Ends become means, and means become ends. For example, the war plans of the great powers in July 1914 contributed to a shared self-fulfilling prophecy among leaders in Berlin, St. Petersburg, and Vienna that only by prompt mobilization and attack could they avoid decisive losses in war. The policymakers found that the structure of the mobilization timetables was not flexible enough for slowing down the momentum of late July and early August toward an irrevocable decision in favor of war.

One result of compressing decision time in a crisis, compared to typical peacetime patterns, is that the likelihood of Type I (undetected attack) and Type II (falsely detected attack) errors increases. Tactical warning and intelligence networks grow accustomed to the routine behavior of other states' forces and may misinterpret nonroutine behavior. Unexpected surges in alert levels or uncharacteristic deployment patterns could trigger tactical operators to misread the indicators. As Bruce G. Blair has argued, "In fact, one distinguishing feature of a crisis is its murkiness. By definition, the Type I and Type II error rates of the intelligence and warning systems rapidly degrade. A crisis not only ushers in the proverbial fog of crisis symptomatic of error-prone strategic warning but also ushers in a fog of battle arising from an analogous deterioration of tactical warning."[8]

A third attribute of successful crisis management is that each side should be able to offer the other a safety valve or a face-saving exit from a predicament that has escalated beyond expectations. In some cases, a graceful or cost-beneficial exit may not be available to either side; it will then become a competition in minimizing risk. The search for options should not back either crisis participant into a corner from which there is no graceful retreat. For example, during the Cuban missile crisis of 1962, President Kennedy was able to offer Soviet Premier Khrushchev a face-saving exit from his overextended missile deployments. Kennedy publicly committed the United States to refrain from future military aggression against Cuba and privately agreed to remove and dismantle Jupiter medium-range ballistic

8 Bruce G. Blair, *The Logic of Accidental Nuclear War* (Washington: Brookings Institution, 1993), p. 237.

missiles previously deployed among the United States' NATO allies.[9] After some days of deliberation and having a clearer focus of the Soviet view of events, Kennedy and his inner circle recognized that publicly humiliating Khrushchev would cause the United States to lose and not gain, which in turn could diminish Khrushchev's interest in achieving any mutual agreement to resolving the crisis.

A fourth characteristic of successful crisis management is that each side maintains an accurate perception of the other side's intentions and military capabilities, including the opponent's susceptibilities and vulnerabilities. For example, posturing as if one is willing to escalate to war can sometimes terminate a crisis on favorable terms. Estimating opponents' intentions and capabilities becomes difficult during a crisis, however, because intentions and capabilities can change in the heat of a partly competitive relationship and a threat-intensive environment. Robert Jervis warned that beliefs in the inevitability of war during the Cold War might have created a self-fulfilling prophecy, writing that, "The superpowers' beliefs about whether or not war between them is inevitable create reality as much as they reflect it. Because preemption could be the only rational reason to launch an all-out war, beliefs about what the other side is about to do are of major importance and depend in large part on an estimate of the other's beliefs about what the first side will do."[10]

Intentions can shift during a crisis if policymakers become more optimistic about gains or more pessimistic about potential losses. The management of military alerts and the deployment or other movement of military forces can change capabilities. Heightened states of military readiness on each side are intended to send a two-sided signal: of readiness for the worst if the other side attacks and of a nonthreatening steadiness of purpose in the face of enemy passivity. This mixed message is hard to relay under the best of crisis management conditions, since a state's behaviors and communications may seem inconsistent as observed by its opponent. Under the stress of time pressures and military threats, different wings of complex security organizations may make decisions from the perspective of their narrowly defined, bureaucratic interests. These decisions and actions may

9 Lebow and Stein, *We All Lost the Cold War*, pp. 122–23.

10 Robert Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon* (Ithaca: Cornell University Press, 1989), p. 183.

not reflect the policymakers' intent or may not be done in coordination with the decisions and actions of other parts of government. As Alexander L. George has explained,

> It is important to recognize that the ability of top-level political authorities to maintain control over the moves and actions of military forces is made difficult because of the exceedingly large number of often complex standing orders that come into effect at the onset of a crisis and as it intensifies. It is not easy for top-level political authorities to have full and timely knowledge of the multitude of existing standing orders. As a result, they may fail to coordinate some critically important standing orders with their overall crisis management strategy.[11]

As policymakers may be challenged to control numerous and diverse standard operating procedures, political leaders may also be insensitive to the costs of sudden changes in standing orders or unaware of the rationale underlying those orders. For example, heads of state or government may not be aware that more permissive rules of engagement for military forces operating in harm's way often come into play once higher levels of alert have been authorized.[12] In other cases, however, control is fairly tight. Crisis managers soon learn on the job an important lesson about the distinction between a crisis and an actual outbreak of war: The jump from one to another is less of a dichotomy than it is a continuum, and the end stage of crisis is not obvious until the fateful steps into war have been irrevocably taken. For example, heads of state in Europe in 1914 were at first overconfident in their ability to manage a crisis short of war, but as events gradually eluded them, they became more fatalistic in a self-defeating manner.

Potential Disrupters

Information or cyber warfare has the potential to attack or to disrupt successful crisis management on each of the preceding attributes.[13] First, cyber warfare

11 Alexander L. George, "The Tension Between 'Military Logic' and Requirements of Diplomacy in Crisis Management," in *Avoiding War: Problems of Crisis Management*, pp. 13–21, citation p. 18.

12 George, "Tension Between Military Logic and Requirements of Diplomacy."

13 For useful definitions of cyberattack and cyberwar, see Paul K. Davis, "Deterrence, Influence, Cyber Attack, and Cyberwar," *International Law and Politics* 47 (2015): 327–355.

can muddy the signals being sent from one side to the other during a crisis. This can be done deliberately or inadvertently. Suppose one side plants a virus or worm in the other's communications networks.[14] The virus or worm becomes activated during the crisis and destroys or alters information. The missing or altered information may make it more difficult for the cyber victim to arrange a military attack. But destroyed or altered information may mislead either side into thinking that its signal has been correctly interpreted when it has not. Thus, side A may intend to signal "resolve" instead of "yield" to its opponent on a particular issue. Side B, misperceiving a "yield" message, may decide to continue its aggression, meet unexpected resistance, and cause a much more dangerous situation to develop. There is also the possibility of cyber-enabled preemption to disable enemy nuclear missiles before they reach the launch pad or during the launch itself. The United States apparently has used such "left-of-launch" techniques against North Korea.[15] During a nuclear crisis, would such a move be accepted by the attacked party as one of intimidation and deterrence? Or on the contrary, would offensive cyberwar against missile launches prompt a nuclear first use or first strike by the defender out of fear of losing its retaliatory capability?

Cyberwar can also destroy or disrupt communication channels necessary for successful crisis management. It can disrupt communication links between policymakers and military commanders during a period of high threat and severe time pressure. This disruption might not be altogether intentional but could result from having earlier implanted malware that activated either unexpectedly or without the full control of its creators. From the standpoint of civil-military relations, two kinds of unanticipated problems are possible under these conditions. First, political leaders may have pre-delegated limited authority for nuclear release or launch under restrictive conditions:

14 A virus is a self-replicating program intended to destroy or alter the contents of other files stored on floppy disks or hard drives. Worms corrupt the integrity of software and information systems from the "inside out" in ways that create weaknesses exploitable by an enemy.

15 David E. Sanger and William J. Broad, "Trump Inherits a Secret Cyberwar Against North Korean Missiles," *New York Times*, March 4, 2017, https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html?_r=0. See also, Jesse T. Wasson and Christopher E. Bluesteen, "Taking the Archers for Granted: Emerging Threats to Nuclear Weapon Delivery Systems," (Paper presented at the Annual Conference of International Studies Association, Baltimore, MD, 2017).

Only when these few conditions are met, according to the protocols of pre-delegation, would military commanders be authorized to employ nuclear weapons distributed within their command. Clogged, destroyed, or disrupted communications could prevent the leaders from knowing that military commanders have perceived a situation far more desperate than it really is, and thus permissive of nuclear initiative. For example, during the Cold War, disrupted communications between the US National Command Authority and ballistic missile submarines, once the latter came under attack, could have led submarine officers and crew to jointly decide to launch in the absence of contrary instructions.

Critical reviewers of an earlier draft of this article pointed out correctly that it seemed paradoxical to assume that leaders would authorize cyberwar during a crisis that they would otherwise prefer to terminate before it resulted in war. It would make more sense, at least in principle, to conduct cyberwar in conjunction with a first strike but not before it. I concede the logic, but it has another side. First, cyberattacks during a crisis might not only be a means of creating technical glitches in the enemy's information systems and decision-making process but could also be a form of strategic bargaining for a more advantageous conflict termination or—if it came to that—a more favorable war outcome. For example, "left-of-launch" techniques for disrupting the networks that support missile launch systems could support one side's antimissile defense capabilities and increase the other side's self-doubts about favorable performance of its ballistic missile attacks.

Second, information warfare during a crisis will almost certainly increase the time pressure in which political leaders operate. It may do this literally or it may affect the perceived time frame during which the policymakers can make their decisions. Once either side sees parts of its command, control, and communications system being subverted by phony information or extraneous cyber-noise, its sense of panic at the possible loss of military options will be enormous. In the case of the United States' strategic nuclear war plan (SIOP) during the Cold War, for example, disruption of even portions of the strategic command, control, and communications system could have prevented competent execution of parts of the SIOP. The SIOP depended upon finely orchestrated time-on-target estimates and precise damage expectancies against various classes of targets. Partially misinformed or disinformed networks and communications centers would have caused redundant attacks against the

same target sets and, quite possibly, unplanned attacks on friendly military or civilian installations.

A third potentially disruptive effect of information warfare on nuclear crisis management is that it may reduce the search for available alternatives among the few and desperate. Policymakers searching for escapes from crisis denouements need flexible options and creative problem solving. Victims of cyber warfare may have a diminished ability to routinely solve problems, let alone creatively, once information networks are filled with flotsam and jetsam. Questions to operators will be poorly posed, and responses (if available at all) will be driven toward the least common denominator of previously programmed standard operating procedures. Retaliatory systems that depend on launch-on-warning instead of survival after riding out an attack are especially vulnerable to reduced-time cycles and restricted alternatives. As Blair states, "A well-designed warning system cannot save commanders from misjudging the situation under the constraints of time and information imposed by a posture of launch-on-warning. Such a posture truncates the decision process too early for iterative estimates to converge on reality. Rapid reaction is inherently unstable because it cuts short the learning time needed to match perception with reality."[16]

The propensity to search for the first available alternative that meets minimum satisfactory conditions of goal attainment is strong enough under normal conditions within nonmilitary bureaucratic organizations.[17] In civil-military command and control systems under the stress of nuclear crisis decision-making, the first available alternative may quite literally be the last, or so policymakers and their military advisors may persuade themselves. Accordingly, the bias toward prompt and adequate solutions is great. During the Cuban missile crisis, for example, members of the presidential advisory group continued to propound an air strike and invasion of Cuba during the entire thirteen days of crisis deliberation. Had less time been available for debate and had President Kennedy not deliberately structured the discussion in a way that forced alternatives to rise to the surface, the air strike and invasion might well have been the chosen alternative.[18] As Paul K. Davis has

16 Blair, *The Logic of Accidental Nuclear War*, p. 252.

17 James G. March and Herbert A. Simon, *Organizations* (New York: John Wiley and Sons, 1958), pp. 140, 146.

18 Lebow and Stein, *We All Lost the Cold War*, pp. 335–336.

noted, "Usual discussions of crisis stability assume that leaders are in control of their nuclear capabilities. Again, history is sobering. President Kennedy became worried in 1961 about possible unilateral actions by military leaders to prepare a preemptive strike against the Soviet Union. He instigated efforts to tighten the President's personal control. Soviet leadership worried about survivability of its forces and developed capability for launch on warning and automated response. Such systems could be the source of accidental war."[19]

Finally, cyberwar can cause each side to convey flawed images of its intentions and capabilities, with potentially disastrous results. Another example from the Cuban missile crisis demonstrates the possible side effects of simple misunderstanding and noncommunication in US crisis management. At the most tense period of the crisis, a U-2 reconnaissance aircraft got off course and strayed into Soviet airspace. US and Soviet fighters scrambled, and a possible Arctic confrontation of air forces loomed. Khrushchev later told Kennedy that Soviet air defenses might have interpreted the U-2 flight as a prestrike reconnaissance mission or as a bomber, calling for a compensatory response by Moscow.[20] Fortunately, Moscow chose to give the United States the benefit of the doubt in this instance and permitted US fighters to escort the wayward U-2 back to Alaska. Why this scheduled U-2 mission was not scrubbed once the crisis began has never been fully revealed; the answer may be as simple as bureaucratic inertia compounded by noncommunication down the chain of command by policymakers who failed to appreciate the risk of "normal" reconnaissance under these extraordinary conditions.

The assessment below of expert analyst Martin Libicki on the relationship between cyberwar and crisis management underscores the preceding discussion and examples:

> To generalize, a situation in which there is little pressure to respond quickly, in which a temporary disadvantage or loss is tolerable, and in which there are grounds for giving the other side some benefit of the doubt is one in which there is time for crisis management

19 Paul K. Davis, Peter Wilson, Jeongeun Kim, and Junho Park, "Deterrence and Stability for the Korean Peninsula," *Korean Journal of Defense Analysis* no. 1 (March 2016): 14.

20 Graham T. Allison, *Essence of Decision: Explaining the Cuban Missile Crisis* (Boston: Little, Brown, 1971), p. 141. See also Scott D. Sagan, *Moving Targets: Nuclear Strategy and National Security* (Princeton: Princeton University Press, 1989), p. 147; and Lebow and Stein, *We All Lost the Cold War*, p. 342.

> to work. Conversely, if the failure to respond quickly causes a state's position to erode, a temporary disadvantage or degree of loss is intolerable, and there are no grounds for disputing what happened, who did it, and why—then states may conclude that they must bring matters to a head quickly.[21]

Scenarios and Risks

The outcome of a nuclear crisis management scenario influenced by information operations may not be a favorable one. Despite the best efforts of crisis participants, the dispute may degenerate into a nuclear first use or first strike by one side and retaliation by the other. In that situation, cyber operations by either or both sides might make it more difficult to limit the war and end it before catastrophic destruction and loss of life has taken place. As in the prior discussion, the specifics of each case matter. In psychological warfare, attackers and the recipients of their attacks may intentionally misrepresent successes as failures or vice-versa if such misrepresentation contributes to a preferred outcome of de-escalation. Although "small" nuclear wars do not exist, there is an opposite view as well; during the Cold War, the notion of limited nuclear warfare, tactical nuclear warfare, or limited exchanges was developed, and similar ideas also floated around India-Pakistan. Compared to conventional wars, there can be different kinds of "nuclear" wars, in terms of their proximate causes and consequences.[22] Possibilities include a nuclear attack from an unknown source; an ambiguous case of possible but not proven nuclear first use; a nuclear "test" detonation intended to intimidate but with no immediate destruction; or, a conventional strike mistaken at least initially for a nuclear one. As George H. Quester has noted, "The United States and other powers have developed some very large and powerful conventional warheads, intended for destroying the hardened underground bunkers that may house an enemy command post or a hard-sheltered weapons system. Such 'bunker-buster' bombs radiate a sound signal when they are used and an underground seismic signal that could be mistaken from a distance for the signature of a small nuclear warhead."[23]

---

21 Martin C. Libicki, *Crisis and Escalation in Cyberspace* (Santa Monica: RAND Corporation, 2012), p. 145.

22 For pertinent scenarios, see George H. Quester, *Nuclear First Strike: Consequences of a Broken Taboo* (Baltimore: Johns Hopkins University Press, 2006), pp. 24–52.

23 Quester, *Nuclear First Strike*, p. 27.

The dominant scenario of a general nuclear war between the United States and the Soviet Union preoccupied Cold War policy makers, and as a result, concerns about escalation control and war termination were swamped by apocalyptic visions of the end of days. The second nuclear age, roughly coinciding with the end of the Cold War and the demise of the Soviet Union, offers a more complicated menu of nuclear possibilities and responses.[24] Interest in the threat or use of nuclear weapons by rogue states, by aspiring regional hegemons or by terrorists, abetted by the possible spread of nuclear weapons among currently non-nuclear weapons states, stretches the ingenuity of military planners and fiction writers.

In addition to the world's worst characters engaged in nuclear threat or first use, backsliding is also possible, depending on the political conditions between the United States and Russia, or Russia and China, or China and India (among current nuclear weapons states). The nuclear "establishment" or P-5 thus includes cases of current debellicism or pacification that depend upon the continuation of favorable political auguries in regional or global politics. Politically unthinkable conflicts of one decade have a way of evolving into the politically unavoidable wars of another—World War I is instructive in this regard. The war between Russia and Georgia in August, 2008 was a reminder that local conflicts along regional fault lines between blocs or major powers could expand into worse conflicts, as was the case also

24 Assessments of deterrence before and after the Cold War appear in Colin S. Gray, *The Future of Strategy* (Cambridge: Polity Press, 2015), pp. 98–106; Paul Bracken, *The Second Nuclear Age: Strategy, Danger, and the New Power Politics* (New York: Henry Holt—Times Books, 2012); Adam B. Lowther, ed., *Deterrence: Rising Powers, Rogue Regimes, and Terrorism in the Twenty-First Century* (New York: Palgrave Macmillan, 2012); Beatrice Heuser, *The Evolution of Strategy: Thinking War from Antiquity to the Present* (Cambridge: Cambridge University Press, 2010), pp. 351–383; Michael Krepon, *Better Safe than Sorry: The Ironies of Living with the Bomb* (Stanford: Stanford University Press, 2009); Lawrence Freedman, *Deterrence* (Cambridge: Polity Press, 2004); Lawrence Freedman, *The Evolution of Nuclear Strategy,* 3rd ed. (New York: Palgrave Macmillan, 2003); Patrick M. Morgan, *Deterrence Now* (Cambridge: Cambridge University Press, 2003); Keith B. Payne, *The Fallacies of Cold War Deterrence and a New Direction* (Lexington: University Press of Kentucky, 2001); Colin S. Gray, *The Second Nuclear Age* (Boulder: Lynne Rienner, 1999); Keith B. Payne, *Deterrence in the Second Nuclear Age* (Lexington: University Press of Kentucky, 1996); and Robert Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon* (Ithaca: Cornell University Press, 1989).

in the Balkan wars in the 1990s. In these cases, Russia's one-sided military advantage relative to Georgia in 2008 and NATO's military power vis-à-vis that of Bosnians of all stripes in 1995 and Serbia in 1999 contributed to terminating war without further international escalation.

Escalation of a conventional war into nuclear first use remains possible where operational or tactical nuclear weapons have been deployed with national or coalition armed forces. In allied NATO territory, the United States deploys several hundred sub-strategic, air delivered nuclear weapons among bases in Belgium, Germany, Italy, the Netherlands, and Turkey.[25] Russia likely retains several thousands of operational or tactical nuclear weapons, including significant numbers deployed in western Russia.[26] The New START agreement, once ratified, establishes a notional parity between the United States and Russia in nuclear systems of intercontinental range.[27] But the superiority of the United States and the allied NATO in advanced technology, information-based conventional military power leaves Russia heavily reliant on tactical nukes as compensation for its comparative weakness in non-nuclear forces. NATO's capitals breathed a sigh of relief when Russia's officially-approved Military Doctrine of 2010 did not seem to lower the bar for nuclear first use, compared to previous editions.[28]

---

25 For background on US tactical nuclear weapons deployed in Europe, see Hans M. Kristensen, *U.S. Nuclear Weapons in Europe: A Review of Post-Cold War Policy, Force Levels, and War Planning* (Washington, DC: Natural Resources Defense Council, February 2005).

26 See Pavel Podvig, "What to do about tactical nuclear weapons," *Bulletin of the Atomic Scientists*, February 25, 2010, https://thebulletin.org/2010/02/what-to-do-about-tactical-nuclear-weapons/ and Jacob W. Kipp, "Russia's Tactical Nuclear Weapons and Eurasian Security," *Eurasia Defense Monitor*, March 5, 2010, https://jamestown.org/program/russias-tactical-nuclear-weapons-and-eurasian-security/.

27 "Treaty between the United States of America and the Russian Federation on Measures for the Further Reduction and Limitation of Strategic Offensive Arms" (Washington, DC: US Department of State, April 8, 2010), http://www.state.gov/documents/organization/140035.pdf.

28 "The Military Doctrine of the Russian Federation," February 5, 2010, in *Johnson's Russia List* 2010, #35, February 19, 2010. See also Nikolai Sokov, "The New, 2010 Russian Military Doctrine: The Nuclear Angle," *Center for Nonproliferation Studies, Monterey Institute of International Studies*, February 5, 2010, http://cns.miis.edu/stories/100205_russian_nuclear_doctrine.htm.

Russia's military doctrine indicates a willingness to engage in nuclear first use in situations of extreme urgency, as defined by its political leadership.[29] And, despite evident superiority in conventional forces relative to those of Russia, neither the United States nor NATO is necessarily eager to get rid of their remaining sub-strategic nukes deployed among American NATO allies. An expert panel convened by NATO to set the stage for its 2010 review of its military doctrine was carefully ambivalent about NATO's forward deployed nuclear weapons. The issue of negotiating away these weapons in return for parallel concessions by Russia was left open for further discussion. On the other hand, the NATO expert report underscored the present sentiment of the majority of governments that these weapons provided a necessary link in the chain of alliance deterrence options.[30]

Imagine now the unfolding of a nuclear crisis or the making a decision for nuclear first use, under the conditions of both NATO and Russian campaigns employing strategic disinformation and information operations intended to disrupt enemy command-control, communications, and warning systems. Disruptive cyber operations against enemy systems on the threshold of nuclear first use, or shortly thereafter, could increase the already substantial difficulty of halting the fighting before a European-wide theater conflict or a strategic nuclear war occurs. The above cited difficulties in crisis management, under the shadow of nuclear deterrence and pending a decision for first use, would place the cohesion of allied governments under unprecedented stress and danger, undoubtedly aided by a confused situation on the battlefield.

NATO would be subjected to three new kinds of friction. First, the decision to use nuclear weapons falls solely within the US (or UK/French) chain of command. NATO has insufficiently considered the challenge of managing a decision-making process on the brink of war among the twenty-nine member states in the alliance, compared to the sixteen members during the Cold War years. The number of member states is not only larger but the diversity of their foreign policy and national security priorities—as well as their variable military-political doctrines—represents a formidable obstacle

29 See the analysis by Keir Giles, *The Military Doctrine of the Russian Federation 2010*, *NATO Research Review* (Rome: NATO Defense College, Research Division, February 2010), esp. pp. 1–2 and 5–6.

30 NATO, *NATO 2020: Assured Security; Dynamic Engagement, Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO* (Brussels: North Atlantic Treaty Organization, May 17, 2010), pp. 43–44.

in making decisions under duress, especially for nuclear first use. Second, reliable intelligence about Russian intentions following Russian or NATO first use would be essential but challenging to nail down. Third, the first use of a nuclear weapon in anger since Nagasaki would establish a new psychological, political, and moral universe in which negotiators seeking de-escalation and termination of war would somehow have to maintain their sangfroid, convince their militaries to agree to stand down, and return nuclear-capable launchers and weapons to secured but transparent locations. All of this would take place within the panic spread by the 24/7 news networks and the internet.

Conclusion

The possible combination of information warfare with continuing nuclear deterrence after the Cold War could have unintended by-products, and these may be dangerous for stability. One possible objective of cyberwar in conventional warfare could be to deny enemy forces battlespace awareness and to obtain dominant awareness for oneself, as the United States largely was able to do in the Gulf War of 1991.[31] In a crisis in which nuclear weapons are available to the side under cyberattack, crippling the foe's intelligence and command and control systems is an objective possibly at variance with controlling conflict and prevailing at an acceptable cost. And under some conditions of nuclear crisis management, crippling the C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) of the opponent may be self defeating. Deterrence, whether it is based on the credible threat of denial or retaliation, must be successfully communicated to—and believed by—the other side.[32]

31 As David Alberts notes, "Information dominance would be of only academic interest, if we could not turn this information dominance into battlefield dominance." See Alberts, "The Future of Command and Control with DBK," in *Dominant Battlespace Knowledge*, ed. Stuart E. Johnson and Martin C. Libicki (Washington: National Defense University, 1996), p. 80, and also pp. 77–102.

32 As Colin S. Gray has noted, "Because deterrence flows from a relationship, it cannot reside in unilateral capabilities, behavior or intentions. Anyone who refers to *the* deterrent policy plainly does not understand the subject." Gray, *Explorations in Strategy* (Westport: Greenwood Press, 1996), p. 33.

Broad Economic Warfare in the Cyber Era

Shmuel Even

Broad economic warfare encompasses a host of actions aimed at damaging or threatening to damage the economy of an enemy or rival, with the aim of pressuring or weakening it in order to achieve strategic aims. Broad economic warfare encompasses standard economic warfare (such as sanctions), kinetic warfare, and cyber warfare against an enemy's economy. The cyber era has changed the realm of broad economic warfare. From an offensive perspective, cyber capabilities make it possible to damage the enemy economy both during wartime and between wars. Cyber warfare can intensify the damage caused to an enemy's economy by economic sanctions and/or kinetic attacks. From a defensive perspective, cyber warfare poses another danger to the functioning of the economy. Although extreme scenarios of cyberattacks against the economies of countries have not occurred yet, it is necessary that the pace of building defenses for the state cyber system adapt to the rapidly accelerating establishment of the economy within the cybersphere.

Keywords: Broad economic warfare, economics, warfare, cyber, Israel, Iran

Dr. Shmuel Even is a senior research fellow at the Institute for National Security Studies.

Introduction

The purpose of this article is to present the concept of broad economic warfare and explore its application in the cybersphere. The article is divided into two parts. The first part defines broad economic warfare as encompassing all acts of warfare that target the enemy's economy. This field encompasses standard economic warfare (such as sanctions), kinetic warfare, and cyber warfare against an enemy economy. It is also characterized by defensive aspects. The second part of the article focuses on cyber warfare as one means of broad economic warfare and distinguishes between soft and hard warfare. The article discusses examples of different ways of implementing this kind of warfare.

Background

Strategies of warfare that are economic in character have been around since ancient times. In those days, the blockade was a common implement of warfare and the spoils of war constituted the supplies that advancing armies required and the remuneration enjoyed by the victors. Strategies of economic warfare have evolved since then, resulting from changes in the world's economic, political, and military realities. *Encyclopedia Britannica* defines economic warfare as "the use of, or the threat to use, economic means against a country in order to weaken its economy and thereby reduce its political and military power."[1] According to the *Oxford Dictionary*, economic warfare is "an economic strategy based on the use of measures (e.g., blockade) of which the primary effect is to weaken the economy of another state."[2]

It has been typical, at least in recent decades, to view standard economic warfare as limited to measures that do not use military force against the economy of the enemy; that is, attacking the economy of an enemy state using kinetic weapons in order to impair the production capacity of the enemy is not part of the toolbox of standard economic warfare. However, the use of the blockade, which is a military implement that could lead to the use of kinetic weapons within the framework of standard economic warfare, is somewhat ambiguous. This issue has also raised questions about

1 George Shambaugh, "Economic Warfare," *Encyclopedia Britannica*, https://www.britannica.com/topic/economic-warfare.

2 "Economic war," *Oxford Dictionaries*, https://en.oxforddictionaries.com/definition/economic_war.

the classification of high-intensity cyberattacks against economic targets of the enemy, of which the expected results are no less powerful than kinetic attacks. This includes, for example, cyberattacks against power stations, industrial plants, and transportation systems, damage to which is liable to have a kinetic effect (including the destruction of property and loss of life). In an analogy to kinetic attacks, therefore, cyberattacks of this kind are not found in the standard definition of economic warfare.

Given the above, we use the term "broad economic warfare" as a framework to encompass all the different kinds of measures designed to damage—or threaten to damage—the economy of an enemy or rival so that the party exercising the warfare can achieve its strategic aims. The distinction between broad economic warfare and standard economic warfare is summarized in the following table. As noted, broad economic warfare also has a defensive aspect.

Table 1. Broad Economic Warfare vs. Standard Economic Warfare

Category		Characteristic Measures
Economic Warfare (standard definition)		Various kinds of economic sanctions, such as the freezing of assets abroad, proscriptions in commerce and investments, discriminatory trade terms (not based solely on purely economic considerations), boycotts in various economic areas, embargos, and blockades aimed at preventing the enemy from engaging in trade.[3]
Broad economic warfare	**Soft Warfare**	Various kinds of economic sanctions, including freezing assets abroad, boycott, prohibition of trade, and embargo (not including kinetic damage to means of transport of the enemy). A downgrading of the conditions of economic relations with a rival for reasons that are not solely economic in nature, for example, in the realm of trade and investments. Information warfare and "soft" cyber warfare. Use of illegitimate means to achieve a strategic advantage, such as the large-scale theft of intellectual property.
	Hard Warfare	Closure/blockade using military forces aimed at preventing trade by the enemy, which may result in a military confrontation. Kinetic attacks on targets within the enemy economy. High-intensity cyberattacks against infrastructure and factories.

3 *Encyclopedia Britannica.*

Broad Economic Warfare: Definition, Attributes, and Goals

As already noted, broad economic warfare can be defined as measures aimed at harming, or threatening to harm, the economy of an enemy or rival,[4] to exert pressure on it or weaken so that the party exercising the warfare can achieve its strategic aims. This array also includes measures for defending against offensive actions taken by the enemy. In other words, broad economic warfare is a combined field encompassing all the measures of warfare that target the economy of the enemy. It includes sanctions, information warfare, boycott, embargo, military closure, kinetic warfare, and cyber warfare against the enemy's economy. It also includes defensive actions against such measures, such as the capability to respond, measures in preparation for sanctions, passive and active defense, and cyber defense of the economy.

According to the above definition, broad economic warfare is not limited to the standard tools of economic warfare but rather augments them with powerful kinetic and cyberattacks against targets within the enemy's economy. For example, measures against the enemy's electricity system may include ceasing the sale of electricity as a political sanction; sanctions on the import of spare parts for power stations; a cyberattack or kinetic attack that results in a temporary electrical outage; or a high-intensity cyber or kinetic attack that does irreversible damage to the turbine of a power station.

Broad economic warfare may be combined, in part or in full, with other types of measures depending on the goals, means, and strategy adopted. It may be part of "soft" warfare, such as combined with economic sanctions and cyberattacks on an economy with the goal of exerting heavy strategic pressure on the enemy without using military force. It may also be part of "hard" warfare and be carried out alongside high-intensity kinetic attacks and cyberattacks against the enemy's economic targets.

The goals of broad economic warfare are as follows:

1. To exert strategic economic pressure on an enemy or rival in order to change its behavior as desired by the party that is exercising the warfare.
2. To make it difficult to supply resources for the enemy's military buildup with the aim of weakening its force ("force design") and to damage the

4 For example, US president Donald Trump defined Russian president Vladimir Putin not as an enemy but as a rival, after the United States imposed sanctions on Russia. See "Trump Claims Victory in NATO: England will do something," *Ynet*, July 12, 2018, https://www.ynet.co.il/articles/0,7340,L-5308872,00.html [Hebrew].

enemy's economic resources, infrastructure, and assets in order to impair its military activity ("force use").

3. To undermine the status and stability of the enemy regime, to exert pressure on it to bring about a change in its priorities and policy (for example, in the case of the Iranian nuclear program), to strengthen the opposition against it, and even to bring about its overthrow.
4. To deter war or shorten its duration, to exact a price of war from the enemy, and to extend the time it takes it to rebuild itself in the aftermath—with the aim of delaying the outbreak of the next war.
5. To use the enemy's resources against it, or as compensation from it (for example, seizing funds in order to compensate the victims of terrorism).

The Means and Tools of Broad Economic Warfare

Broad economic warfare is divided into two categories: "soft" warfare, which does not make any direct use of kinetic force or the destructive force of cyber; and "hard" warfare, which involves different kinds of force, the intensity of which deviates from soft warfare.

Means of "Soft" Warfare

Soft warfare refers to economic warfare conducted by a single country or a group of countries, as well as organizations, with the aim of exerting significant economic and political pressure on a rival or enemy in order to weaken it and cause it to change its policy, without using military force.

Punitive Measures

These measures include sanctions, embargos, and/or boycotts of the economy of an enemy or rival, such as reducing or suspending economic relations (trade, banking, tourism, investments, and different types of economic agreements); imposing discriminatory import taxes for political reasons; pressuring companies and other countries to halt their economic relations with the enemy or rival country; distancing a recalcitrant country from the mechanisms of the international economy; and freezing the country's funds and assets held abroad. Examples of these measures include comprehensive sanctions imposed against Iran (including the ban on the export of Iranian

oil)[5] and against North Korea[6] due to their nuclear programs; US sanctions imposed on Russia due to its intervention in the US elections using cyber methods;[7] the freezing of Iraq's assets abroad following its invasion of Kuwait in 1990; the oil embargo imposed by the Arab states in 1974, which was intended to pressure the Western economy by creating an oil shortage and an increase in prices; and the boycott of Israel by the Boycott, Divestment, and Sanctions (BDS) movement.

Beyond the direct impact of punitive measures on the economy, such measures also are able to create an atmosphere of economic strangulation and a sense of no way out for the injured party. Still, researchers are divided as to the effect of sanctions, making it preferable to assess each case separately.[8]

Additional Soft Actions for Impairing a Rival's Economy

Other soft actions include cyberattacks aimed at disrupting sites that are essential to the state administration and the economy of the enemy or rival; information warfare aimed at undermining the strength of its economy (for example, by spreading distressing information regarding the low value of the currency, the weakness of the banking system, the flight of capital, and the shortage of food); interference in the enemy or rival's monetary system (for example, the Nazis' production of counterfeit British pound sterling notes during World War II); and acts of technological and industrial espionage between countries aimed at the large-scale theft of intellectual property in order to change the strategic economic balance between them, even though

5 Today, the sanctions are being imposed by the United States, which withdrew from the nuclear agreement with Iran. See, for example, Tal Schneider, "Everything You Need to Know about the Economic Sanctions to be Imposed on Iran," *Globes*, May 8, 2018, https://www.globes.co.il/news/article.aspx?did=1001235164 [Hebrew].

6 "The UN Unanimously Approves New Sanctions against Pyongyang," *Haaretz*, September 12, 2017, https://www.haaretz.co.il/news/world/america/1.4437072 [Hebrew].

7 Ran Dagoni, "As a Result of the Election Interference: The United States Imposes Sanctions on Russia," *Globes*, March 15, 2018, https://www.globes.co.il/news/article.aspx?did=1001228035 [Hebrew]; Missy Ryan, Ellen Nakashima, and Karen DeYoung, "Obama Administration Announces Measures to Punish Russia for 2016 Election Interference," *Washington Post*, December 29, 2016.

8 For theoretical background on the issue of sanctions, see Nizan Feldman, *In the Shadow of Delegitimization: Israel's Sensitivity to Economic Sanctions*, Memorandum no. 163 (Tel Aviv: Institute for National Security Studies, 2017), chapter 1.

information gathering is not considered an act of war. Broad economic warfare also includes the use of economic powers to weaken the enemy for political and/or military reasons, including the imposition of discriminatory import taxes.

Additional Matters

Many measures are conducted in the global economic realm, both in and outside the framework of agreements between countries, and while one party sometimes benefits and another loses, they should not be considered economic warfare. This stems from the observation that broad economic warfare aims primarily at achieving political and military goals, even if the party exercising the warfare faces economic costs.

From the perspective of the side plotting the war, broad economic warfare is not optimal. In contrast, in economic struggles—including trade wars—one side expects to achieve an economic advantage over its trading partners, some of which are allies, using customary measures of the world economy. One example of this approach is the protective tariffs that the US administration imposed on the companies of the European Union, Canada, and Mexico.

To complete the picture, it is also important to note the positive economic levers of influence. This is the flip side of broad economic warfare, although the goals of these levers are the same as those of the negative levers: to cause states and organizations to conduct themselves in the manner desired by the party using them. These involve the use of economic incentives to further military and political aims and they include aid in the form of grants and loans with comfortable terms, economic agreements, preferential terms of trade, the forgiving and spreading of debts, the conveyance of technologies, and more. Both parties may end up benefiting from the use of economic levers of influence: The party that exercised it enjoys political gain, whereas the other party enjoys economic gain. For example, the different forms of US foreign aid strengthen the Unites States' legitimacy to make demands of the countries receiving its aid.

By definition, economic levers of influence are not weapons. Still, some regard the cessation of economic incentives, the threat of such cessation, or the act of making aid conditional upon achieving political aims either as acts of broad economic warfare or as acts bordering on such warfare. For example, the American administration cut its aid to the Palestinians due

to their failure to cooperate politically with it, and Saudi Arabia links its economic aid to Jordan to its demand that Jordan promote Saudi Arabia's political and security aims, which is topped by the goal of curbing Iranian influence in the Middle East.[9] In addition, during the First Gulf War in 1991, the allies that fought against Iraq provided Egypt with billions of dollars of cash aid and slashed its debts to $25 billion, in exchange for its participation in the war against Saddam Hussein. Syria also received economic aid for taking part in the war.

Means of "Hard" Warfare

Military Blockade

A military blockade refers to the use of military force to prevent or limit the flow of goods and services between the enemy state and the rest of the world with the goal of exerting economic pressure on it, primarily to achieve political and military goals. This measure may sometimes also involve the use of kinetic weaponry.

A distinction can be made between a blockade against a recalcitrant state based on international agreements and rules—such as the international coalition's blockade of Iraq after its invasion of Kuwait in 1990—and the blockade that different states attempt to impose against the shipping routes of other countries as part of a war between them. Examples of the latter include the blockade that Iran imposed against Iraq's oil export routes by attacking oil tankers in the Persian Gulf during the Iraq-Iran War in the 1980s; Egypt's blockade of Israel's shipping routes in the Straits of Tiran in May 1967 (which was one of the main causes of the Six Day War); and Germany's use of submarine warfare to sink the commercial ships of its enemies during World War I and II.

Attacks on Infrastructural and Economic Targets

Attacks or the threat of such attacks on infrastructural and economic targets using kinetic weapons and/or high-power cyberattacks are carried out to weaken and deter the enemy, shorten the duration of the war, deter escalation, and raise the cost of the war. Examples include Israel's deterrence of Hezbollah by means of threatening to attack Lebanon's infrastructure; the US attack

9 Dan Arkin, "Economic Aid on Saudi Terms," *IsraelDefense*, June 13, 2018, http://www.israeldefense.co.il/he/node/34572 [Hebrew].

against Iraqi oil facilities during the First Gulf War; the Israeli Air Force's attack on strategic targets within Egypt and Syria during the Yom Kippur War (oil facilities, government institutions, refineries, and relay stations).

Economic Terrorism

Economic terrorism is the attack or threat of attack by terrorist organizations against a state's economic targets or against its sense of economic security. Examples include Hezbollah's threat to strike at power stations in Israel;[10] the "kite terrorism" launched from the Gaza Strip in the summer of 2018, which burned agricultural crops in the Negev; the theft and destruction of agricultural equipment in Israel for nationalist reasons; and terrorist attacks aimed at impairing tourism in Israel.[11]

Broad economic warfare can also be used against terrorist groups, as in the threat against the economy of a population who supports the organization in question (in the case of semi-state organizations), or damage to their sources of funding and financial systems (as implemented in the case of ISIS).

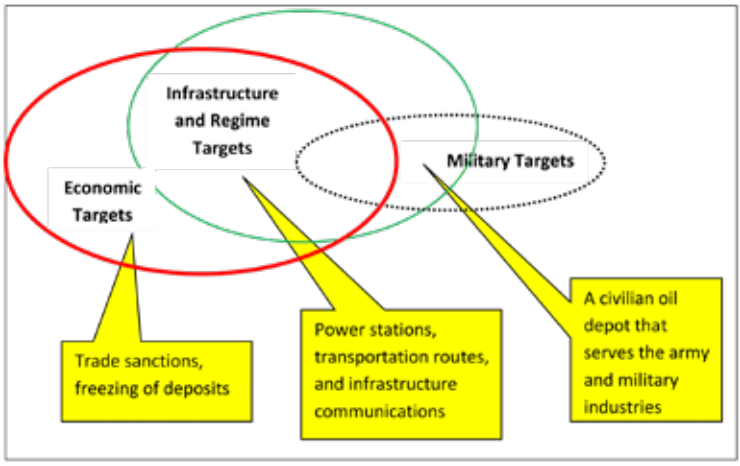

Figure 1. Targets of Attack of Broad Economic Warfare

10 Roy Kais, "Nasrallah: There's no need for chemical weapons, we'll strike at power stations," *Ynet*, September 3, 2012, https://www.ynet.co.il/articles/0,7340,L-4276742,00.html [Hebrew].

11 "From Tourism Destinations to Terrorism Targets: A Concrete Threat against Egypt," *Shorty* (blog), January 14, 2016, http://www.inss.org.il/he/blogs/?pauthor=55226 [Hebrew].

Defense against Broad Economic Warfare

Broad economic warfare also has a defensive aspect. A state's means of defending against such warfare include:

- Deterrence—developing a reliable response capacity and the ability to mount a counter-response;
- Active physical defense—such as the Iron Dome system—and passive defense systems, including the fortification of economic installations;
- The dispersion of infrastructure and strategic economic installations throughout the country; development of the capacity to back up systems and alternative systems, for example, in the realms of communications and energy;
- Cyber defense of the economy (see below);
- Maintenance of reserves of fuel, food, spare parts, and foreign currency in quantities greater than those necessary to meet regular needs;
- Development and maintenance of the ability to self-produce critical products, such as energy (for example, the development of Israel's natural gas fields), food, cement, and so forth;
- Diversification of sources of import in general and critical products in particular, of export destinations, and priority given to long-term contracts with reliable parties who are not influenced by the political conflict in the region;
- Designing of a plan for business continuity in states of emergency, including the development of an ability to recover and to effectively manage the economy during states of emergency, while practicing and providing guidance about this ability prior to declaring states of emergency.

The Advantages and Disadvantages of Broad Economic Warfare

The use of broad economic warfare, of course, has its advantages and its disadvantages. Its advantages include:

- The ability to apply broad economic warfare using a wide spectrum of implements and intensities, such as boycotts, sanctions, blockades, cyberattacks, and kinetic attacks, and to manage and control the campaign until its objectives are met.
- Broad economic warfare can be applied remotely and without many risks to the party exercising it, except for certain kinetic attacks.

- During wartime, broad economic warfare can exert economic pressure upon the enemy to discontinue fighting or to exact an economic price upon the enemy, in order to delay the beginning of the next war while minimizing the loss in human life.
- Broad economic warfare can also be used in campaigns between wars.
- Broad economic warfare, or the threat of its application, can also serve as a deterring factor.

The limitations and dangers of using broad economic warfare include:

- Miscalculation—Use of broad economic warfare may spark or accelerate negative processes and even lead to war. For example, in June 2018, Iran announced the acceleration of its uranium enrichment activities in response to the United States' re-imposition of sanctions against it.[12] From a historical perspective, the economic sanctions that the United States and China imposed on Japan in response to its invasion of China in 1937 resulted in a chain of undesirable outcomes: an alliance between Japan, Nazi Germany, and Italy, followed by Japan's December 1941 attack on Pearl Harbor; and in response to the attack, the United States declared war on Japan, and Japan's allies (including Nazi Germany) declared war on the United States. These developments ultimately resulted in the United States' entry into World War II.
- The population of the enemy country may come to feel hate for the party exercising the broad economic warfare, so that the economic pressure results in popular support of the regime under attack.
- Severe economic pressure could result in large-scale damage to a weak civilian population, which, in turn, could result in a humanitarian crisis and fundamental international criticism.
- Counter-reaction—The rival or enemy could develop an ability to respond using the same implements or others. The outcome could be the evolution of a war in which the assailant also sustains heavy damage.
- Broad economic warfare could result in damage to the assets or economic interests of countries that are friendly or neutral toward the assailant. An example is damage caused to an economic asset in an enemy state, which is ensured by a friendly country, or a computer attack that affects

12 Daniel Salameh and Liad Osmo, "Iran: The Construction of a Facility to Build Advanced Centrifuges Will Be Completed Next Month," *Ynet*, July 7, 2018, https://www.ynet.co.il/articles/0,7340,L-5280313,00.html [Hebrew].

unintended targets. Such incidents are liable to result in counterreactions to the party engaging in the warfare.

Broad Economic Warfare in the Cyber Era

The following is a survey of the overlap between broad economic warfare and the cybersphere.[13] The information and technological revolution that affects the economy and society continues unabated, as the development of computer clouds, big data, augmented reality, artificial intelligence, autonomous vehicles, and "the internet of things" accelerate the reciprocal relations between the economic and social on the one hand, and the cybersphere—which has become increasingly significant in the lives of individuals, organizations, countries, and the world economy—on the other hand.

Today the majority of activity of the economic sector, such as banking and finance, occurs in cyberspace while this sector minimizes its non-digital activity. Although the economic sector is real and tangible, encompassing customers, a work force, land, raw materials, and the products of the metal, building, and food industries (to name a few), all of these are represented in the cybersphere, which documents and links them together, so that a cyberattack affects the entire sector. Another important phenomenon is the globalization of trade and capital markets, which rely on the interlinked internet and cyber systems.

In cyber warfare, the cybersphere is used to damage different enemy targets, with the primary aim of achieving political and military objectives. Cyber warfare may be waged in conjunction with conventional warfare or it can be used on its own. It can be used between wars or during wars, and it can be both defensive and offensive in character. Broad economic warfare uses the cybersphere both to attack economic targets belonging to the enemy, and to defend the country's economic assets and cyber infrastructure, or those connected to the cybersphere itself—for example, factories, power stations, and airports—against enemy cyberattacks.

13 The conceptual expansion of "economic warfare" into "broad economic warfare" also facilitates discussion of powerful cyberattacks that are difficult to include under the standard definition of "economic warfare."

Cyberattacks on the Economy

A cyberattack is an attack against cyber systems that constitute digital infrastructure (for example, organizational software and databases), or an attack carried out by means of cyber (without damaging it) against computer embedded systems operating outside the cybersphere, such as power stations, control towers, traffic light control stations, and so forth. The uniquely offensive aspect of cyber warfare lies in its ability to carry out actions remotely, via cyber, without being directly exposed.[14] In doing so, the attacker does not endanger itself and can follow a policy of ambiguousness (including the avoidance to take responsibility). At times, an attack is not immediately discernible on the surface, and it takes time to be identified (for example, during the disruption of databases).[15]

Cyberattacks against the enemy economy can be carried out in various ways and can be executed at low or high intensity in combination with sanctions or kinetic attacks (using military force). In wartime, cyber has an advantage over kinetic attacks in attacking financial institutions. Cyberattacks can sometimes be used as a substitute for kinetic weapons.

Cyberattacks can serve as an additional means by which terrorist organizations disrupt the way of life in the states they are targeting, particularly given that they can be carried out from anywhere in the world, and not only from close range. Nonetheless, powerful cyberattacks carried out by terrorist groups are still uncommon, although they are expected to increase once terrorist organizations acquire the abilities that enable them to carry out high-intensity cyberattacks with visible results. Furthermore, cyberattacks help—or could help—terrorist organizations acquire funds to pay for their activities. In addition, cyber enables terrorist organizations such as Hezbollah and Hamas to carry out intelligence gathering missions[16] and psychological warfare.

Countries that seek to acquire offensive capabilities have established military cyber organizations. For example, in June 2009 the United States established the US Cyber Command, and in May 2018 this body received

14 These interactions are referred to as non-face-to-face business relationships or transactions.

15 Shmuel Even and David Siman-Tov, *Cyber Warfare: Concepts and Strategic Trends*, Memorandum no. 117 (Tel Aviv: Institute for National Security Studies, 2012).

16 Tal Shahaf, "Hamas's Next Battle Arena: Cyber," *Globes*, April 18, 2018 [Hebrew].

the status of a Unified Combatant Command.[17] Upon its establishment, it announced that the offensive cyber activity against the enemy was meant to create five effects (the five Ds): (1) deny the enemy or rival the ability to operate in cyber; (2) degrade the status of the enemy or rival; (3) disrupt the activity of its systems (4) deceive; and (5) destroy its abilities. These five effects are also relevant to cyber-based broad economic warfare.

Cyber is a platform in which many economic actions are taken, and through these actions, it is possible to intensify economic warfare, such as in the increased enforcement of economic sanctions. Cyber also enables control of the economic realm, for example, by preventing an enemy country from accessing trade and financial systems; blocking the movement of money; preventing the conveyance of trade instructions; implementing information gathering actions and exposing companies that are violating sanctions; freezing and supervising bank accounts; controlling foreign currency across borders through the reports of financial institutions located outside the enemy country; and controlling trade by authenticating data with suppliers outside the enemy country.

Economics by nature is highly sensitive to information, and a significant share of economic systems is based on the public's confidence in the economy and its institutions, such as banks, the national currency, and the systems overseeing the capital markets. Cyber-based broad economic warfare can serve to undermine confidence in the economic systems, including by disseminating relevant information. Still, it is no simple matter to be successful in information warfare of this kind, as cyber also enables the attacked to respond quickly and to refute rumors against it.

Cyberattacks against regime institutions, such as by blocking public access to them, are liable to impair governance and damage the economy and state's income. This is because cyber is a means of establishing a connection between businesses and citizens on the one hand, and government on the other, which has increasingly become a practical—and not only informative—connection, as in the case of paying taxes and fees through websites of governing institutions. Cyber penetration and the gathering of technological and industrial intelligence also enable attackers to acquire a corporation's

17 Ami Rojkes Dombe, "United States Cyber Command Awarded Status of Combatant Command," *IsraelDefense*, May 6, 2018, http://www.israeldefense.co.il/he/node/34080 [Hebrew].

intellectual property. Such actions, when carried out on a significant scale, can change the strategic balance between global corporations, as well as between countries. For example, the United States claims that China carries out such actions in its territory.[18]

Cyberattacks can be managed at a high level of intensity with the aim of disrupting trade, production, and financial activities of the attacked state, such as by damaging databases of trade systems, logistical depots, budgets, and so forth. Such actions are located on the border of "soft" warfare and can also reach higher levels of warfare (depending on the intensity and the scope of the damage). Cyberattacks can be carried out at a higher intensity as part of "hard" warfare. Such attacks are intended to impair the operation of infrastructure and economic systems (electricity, water, banking, transportation, communication), to the point of fundamentally disrupting daily life and the functioning of the enemy state. The ability to remotely damage the functioning of economic systems, without crossing territorial borders and without using military force, is a unique advantage of cyber. At the same time, certain offensive actions carried out in cyber can be disastrous for the country attacked, including loss in human life and damage to essential infrastructure. Such cases are similar to a kinetic attack, and the attacked country's response is liable to be commensurate.

Among the countries that employ cyber to attack economic targets is Iran. In August 2012, Iran was attributed as having carried out a cyberattack against the Saudi national oil company Aramco, using the Shamoon virus. The virus infected some 30,000 computers and impaired the functioning of the company.[19] In 2013, it was reported that Iranian hackers carried out a series of cyberattacks against American targets, including large banks and energy companies operating in the Persian Gulf, but did not result in any significant damage.[20] Another attack using the Shamoon virus, also attributed to Iran, was executed at the end of 2016 against the central bank of Saudi

18 "The United States Accuses China of Stealing $400 Billion in Business Information," *The Marker*, February 17, 2012, https://www.themarker.com/wallstreet/1.1644216?= [Hebrew].

19 Amos Harel, "Assessment: Iran is behind the Cyberattack on the Oil Companies in the Persian Gulf," *Haaretz*, September 11, 2012, http://www.haaretz.co.il/news/world/1.1821619 [Hebrew].

20 "Report: Iran is Conducting an Online Attack against the United States," *Ynet*, October 13, 2013, https://www.ynet.co.il/articles/0,7340,L-4291493,00.html [Hebrew].

Arabia and other state bodies in the kingdom.[21] According to assessments, Iran could respond to US-imposed sanctions with a massive cyberattack.[22] This, however, would expose Iran to the risk of severe retaliation. North Korea, which is also currently subject to sanctions, established a cyberattack apparatus and carries out such attacks primarily against South Korea and Western countries.[23] The above examples indicate that cyber warfare serves as a means of response for countries that are subject to sanctions.

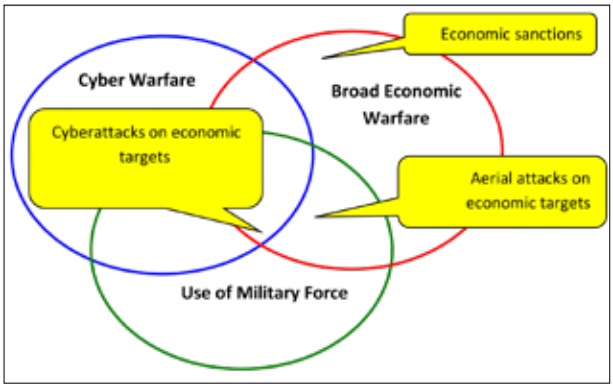

Figure 2. Broad Economic Warfare and Cyber Warfare (Examples)

Defense against Cyberattacks

The Cyber Threat Against the Economy

The state and global economy depends on information systems, databases, communications, and automatization, and their dependence on cyber continues to increase. Today, certain branches of the economy, such as communications and banking, are already deeply entrenched in the cybersphere, and others,

21 "Iranian Hackers Broke into Computers of the Saudi Central Bank," *The Marker*, December 3, 2016, https://www.themarker.com/wallstreet/1.3140741 [Hebrew].

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

23 David E. Sanger, David D. Kirkpatrick, and Nicole Perlroth, "The World Once Laughed at North Korean Cyberpower. No More," *New York Times*, October 15, 2017, https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html.

such as power stations, factories, and transportation operate by means of computer and cyber-embedded systems.

The doomsday scenario of a cyberattack on the economy includes a situation in which banks close; stock market trading ceases; and the operation of power stations, water systems, and transportation enterprises and systems are severely disrupted. According to this scenario, air traffic will cease at airports; factories and offices will close their doors; and foreign trade will come to a standstill. As a result, citizens will have difficulty performing basic actions, such as withdrawing money, receiving their salaries via banks, filling up their gas tanks, buying food at the grocery store, moving from place to place, finding employment, and communicating with government institutions. The government will have difficulty managing the economy and collecting taxes, and all the activity of the economy will grind to a halt. In practice, such broad-scale damage is not necessary to stop the processes of the economy, as striking at a few of its sensitive links is sufficient. So far, however, there has not yet been a cyber event on the doomsday scale, possibly due to the limited abilities of many cyber actors given the defense mechanisms that have been set up by different countries (there is a big difference between a cyber strike on one target or another, and systemic cyber damage to the economy); caution on the part of cyber powers to avoid premature exposure of cyber weapons; fear of countermeasures; and the desire to avoid sparking a cyber arms race and a global cyberwar.[24]

To complete the picture, the most dramatic cyber events in recent years pertaining to national security have occurred in the field of governance in democratic states. For example, the United States maintains that Russia conducted a cyberattack in order to influence the results of the 2016 US presidential election, which has been perceived as a concrete threat to the American democracy. Russia was also accused of trying to interfere in the French presidential elections in 2017 using a similar method—the dissemination on social media of sensitive information against one of the candidates, which it acquired by hacking the computers connected to the

24 Gadi Evron and Boaz Dolev, "War Games: Why the United States is Not Conducting a Cyberattack against North Korea," *Ynet*, September 19, 2017, https://www.ynet.co.il/articles/0,7340,L-5017828,00.html [Hebrew].

candidate.[25] On the other hand, cyber capabilities enabled Turkey's President Recep Erdoğan to thwart a military coup attempt staged against him in July 2016, when he used a cellular application broadcasted to the television and called on his supporters to violate the curfew imposed by the military and to take to the streets.

The state gives preference in terms of cyber defense to its state critical infrastructure (SCI). In Israel, SCI includes electricity infrastructure, water, natural gas, trains, the airport authority, refineries, the electricity production chain and its conduction, government offices, and hospitals. It encompasses twenty-six critical infrastructures that receive instructions directly from the National Cyber Directorate.[26]

The financial sector (banks, credit companies, the credit card clearing system, the capital market, insurance, and pension funds) is particularly sensitive to cyberattacks, due to its critical role in mediating economic and social activities. Unlike heavy industry, the financial sector is more vulnerable to cyberattacks than kinetic attacks. The financial system is based on cyber, sensitive to public confidence, and critical for state functioning. An example of a cyberattack on the financial system was the theft of $81 million in February 2016, when hackers (possibly from North Korea) succeeded in moving funds to the Philippines from the Central Bank in Bangladesh that were held in accounts in the Federal Bank in New York.[27] A similar case of monetary theft took place at a Vietnamese bank at the beginning of 2016. During this event, hackers penetrated the SWIFT system, which is considered to be the most secure interbank payment system in the world.[28] These examples reflect capabilities that can be exercised to a greater extent within the framework of broad economic warfare.

---

25 David Siman-Tov, Gabi Siboni, and Gabrielle Arelle "Cyber Threats to Democratic Processes," *Cyber, Intelligence, and Security* 1, no. 3 (December 2017): 51–63, http://www.inss.org.il/wp-content/uploads/2018/01/CyberENG1.3_6-53-65.pdf.

26 Dan Arkin, "Well Prepared for Threats," *IsraelDefense*, May 24, 2018, http://www.israeldefense.co.il/he/node/34321 [Hebrew].

27 "Operation Lazarus: This is How North Korea Steals Money from Banks in the West through Cyberattack," *Nana*10, April 5, 2017, http://media.nana10.co.il/Article/?ArticleID=1240370 [Hebrew].

28 "Cyberattack on Global Banking: Hackers Again Break into the World's Most Secure Payment System," *The Marker*, May 13, 2016, https://www.themarker.com/wallstreet/1.2942637 [Hebrew].

Other companies in the economy that are sensitive to cyberattacks include those dealing with infrastructure, defense, internet trading, and organizations that make use of sensitive information (law firms, stores of intellectual property, commercial secrets, medical secrets, and so forth). Recent years have witnessed an increasing awareness that organizations' supply chains—the bodies that supply these organizations with intermediate products and with services—constitute an entry point for many of the cyberattacks. This means that defense is required not only of essential targets in the economy but also of the peripheral, surrounding ones as well.

Company employees, including those within the defense industries that deal with the cybersphere, also pose a cyber threat. One example is the serious defense affair that was exposed in July 2018, when an employee of the offensive cyber company NSO was arrested on suspicion that he stole cyber weapons from the company (Pegasus spyware) and attempted to sell them for $5 million. The employee's attempt was thwarted after the "potential buyer" informed the company. This event reflects the need for the state to also supervise what goes on in companies that work in the cybersphere.[29]

Most of the economic damage in the cybersphere up to present has not been caused by broad economic damage by states or organizations but rather by criminals whose primary motivation is financial. Nonetheless, we must assume that everything the criminal sector can do in the cybersphere can also be done by states, which have the capacity to cause even more damage should they choose to wage massive cyber warfare. The 2010 exposure of cyberattacks using the Stuxnet worm that destroyed Iranian centrifuges for the enrichment of uranium illustrates such a powerful state ability.[30] These cyberattacks made it clear to the world that the threat they posed also includes physical damage to industrial plants, infrastructure, and transportation—all of which are equipped with computerized command and control systems—and is not limited solely to damage to databases in the cybersphere.

---

29 Ela Levi-Weinrib and Tal Shahaf, "Permitted for Publication: NSO and One of the Most Serious Cyber Affairs in the History of Israel," *Globes*, July 5, 2018, https://www.globes.co.il/news/article.aspx?did=100124461 [Hebrew].

30 "The Iran File Has Been Opened: Cyber War," Israel Channel 2: *Uvda*, November 2, 2012, https://www.mako.co.il/tv-ilana_dayan/specials/Article-a996bba5fccba31006.htm [Hebrew].

The Response to the Threat

Severe damage to the state's cybersphere should be considered a national security problem. Cyber defense in its economic context involves an array of actions both inside and outside the cybersphere, aimed at defending the state economy against attacks that make use of cyber, both in the cybersphere and in other areas. Cyber defense must be implemented to protect against other states, enemy organizations, crime groups, and malicious actors, as well as to recover from mishaps.

The primary difference between the economic warfare of states that use cyber and criminal activities in this realm is that cyber criminals' motivation is typically criminal and financial (such as the theft of money, commercial secrets, or intellectual property; extortion; collecting ransom).[31] At the same time, however, in some cases, states have related to large-scale cybercrime and even to the unusual economic activities of bodies operating for the sake of profit as threats to their national security.[32]

Whereas border defense and defense of the home front against missiles are the responsibility of the army, defense of the economy's cyber assets—in Israel and around the world—depends primarily upon security services, strategic products of the private sector, and the resources of the sector. A diverse industry of companies produces, markets, and provides support for cyber defense systems.

The need of the private sector—and not of the state— to defend itself against cyber theft of finances, intellectual property, and commercial and technological secrets, as well as cyberattacks motivated by ideological or psychological reasons (ego, vandalism, and so forth) has been the force in

31 Alan Blinder and Nicole Perlroth, "Atlanta Hobbled by Major Cyberattack that Mayor Calls 'a Hostage Situation'," *New York Times*, March 28, 2018, https://www.seattletimes.com/nation-world/atlanta-hobbled-by-major-cyberattack-that-mayor-calls-a-hostage-situation/.

32 For example, at the beginning of 2010, in the midst of the financial crisis in Europe, speculators were marked as "economic terrorists." At the time, the German finance minister said that Germany would consider instructing its intelligence agencies to begin monitoring the organization and activity of speculative investors in order to protect the euro. In addition, the Spanish newspaper *El Pais* reported that Spain's secret service had initiated an investigation of "attacks" on the state by speculators.

developing a cyber defense industry in the local and global economy.[33] The primary role of government security entities in defending the economy lies in its instruction and supervision of prominent bodies of considerable importance. The state is engaged primarily in defending its institutions and instructing organizations that are classified as SCI. At most, the economy and population have the ability to contact the national emergency hotline (CERT) and to access the guide for cyber defense.

Cyber technology is characterized by a rapid pace of change, making it difficult to anticipate how it will look in just another few years. As a result, it is difficult to draw up multi-year programs in the sphere of cyber defense.[34] Rapid change also means high costs of technological depreciation, as things that are installed today will not necessarily be relevant in a few years' time and new versions of software will need to be updated regularly, increasing the dependence on suppliers of technology.

In most cyberattacks, it is difficult to identify the attacker (who takes precautions to conceal his or her identity and to evade detection) and the number of attackers involved; thus, organizations and companies are obligated to adopt broad cyber defense strategies aimed not at specific attackers but rather at various kinds of attacks coming from different sources with increasing level of difficulty, all in order to address the rapid technological developments in the field. Initially, peripheral defense systems were developed, emphasizing defense against remote penetration and the removal of viruses that penetrated the system. However, over the past decade, systems have been developed to halt or deter unauthorized and possibly hostile activity undertaken by someone who physically can penetrate the organization (close contact penetration), including an employee or supplier. Today, physical defense systems, security officers, and the use of manpower selection systems in human resource departments also play important roles in the cyber defense system.

Over the years, the state has made defending infrastructure and the financial sector against cyberattacks a regulatory requirement. In this context, bodies

33 Gabi Siboni and Hadas Klein, "Developing Organizational Capabilities to Manage Cyber Crises," *Cyber, Intelligence, and Security* 2, no. 1 (May 2018): 21–38, http://www.inss.org.il/wp-content/uploads/2018/05/Developing-Organizational-Capabilities-to-Manage-Cyber-Crises.pdf.

34 "From Zion the Cyber Will Come Forth," Product of Israel: A Special Insert for Independence Day, *Haaretz*, April 2018 [Hebrew].

have also been established to engage in cyber defense on a national level. In Israel, for example, a national authority for information security began operating within the General Security Service (GSS) in 2002; in 2011, the National Cyber Directorate was established; in 2015, the National Authority for Cyber Defense was created;[35] and at the end of 2017, the government decided to form a national cyber directorate in the Prime Minister's office, as a merger of the National Cyber Directorate with the National Authority for Cyber Defense.[36] Despite all these measures, Israel still has a long way to go until it achieves full defense of its national cybersphere. As a vision for the future, we can expect the state to assume more practical responsibility in defending the cybersphere of the entire economy and population. Just as the state provides clean water and a steady flow of electricity to both businesses and residences, it should ensure that computer communications are stable and untainted by malware.

Given the above, it is extremely important to integrate the government and the private sectors within the realm of cyber defense. The state needs to integrate the private sector into the national cyber defense activity, both as a major consumer and as a partner in the defense system.[37] One example is the establishment in January 2017 of a banking center for cyber defense in Israel, which was a joint initiative of the National Cyber Defense Authority, the Finance Ministry, Banking Supervision, the banking corporations, and the credit card companies.[38] Israel has an advantage in this area due to its relatively small number of banks, close government supervision, and high levels of cyber capability; still, a minority of banks may be disadvantaged from the perspective of risk diversification.

The fact that cyberspace does not have territorial borders requires international cooperative efforts for national cyber defense. Indeed, at a

35 Ami Rojkes Dombe, "The Cyber Authority Will Replace the GSS in Overseeing Information Security in Banks," *IsraelDefense*, May 9, 2016 [Hebrew].

36 See the website of the National Cyber Directorate at https://www.gov.il/he/Departments/about/newabout [Hebrew].

37 Shmuel Even, "The Strategy for Integrating the Private Sector into National Cyber Defense in Israel," *Military and Strategic Affairs* 7, no. 2 (September 2015): 103–124, http://www.inss.org.il/wp-content/uploads/systemfiles/MASA7-2Eng%20Final_Even.pdf.

38 "A Cyber Banking Center Was Established and Started to Operate in January," *Read it Now*, March 20, 2017, https://www.readitnow.co.il/news [Hebrew].

NATO summit held in July 2018, the leaders of the member states also agreed to increase their countries' preparedness against cyberattacks.[39] In the Israeli context, GSS Director Nadav Argaman maintains that "the State of Israel is currently one of the world's leading cyber power, and this includes the security system and the Israeli intelligence community. We, of course, cooperate with intelligence services and security systems from around the world. As an organization, we have quite a significant cyber capability, both for defense and for offense. We, of course, cooperate with the overall Israeli security system and do nothing alone. We have extremely broad capabilities."[40]

An example of international cooperation in the financial sphere is the Financial Action Task Force (FATF),[41] which was established in 1989 to develop and promote a policy to fight money laundering and the funding of terrorism and weapons of mass destruction. Despite their differences, these areas all deal with finances from sources that are intended to be hidden, and the means of dealing with them are similar. This organization has pointed out that one of the risks in the cyber era is the ability to conduct illegal transactions and to use unlawful funds in cyber, without the direct (face-to-face) exposure of the person performing the action. The FATF also issued a list of criteria according to which states that are not members of its framework will be checked, and if it is decided that they do not meet the criteria, they could be placed on a blacklist that allows them to be subjected to heavy sanctions.

The risk posed by transferring unlawful funds has increased in recent years along with the emergence of the use of Bitcoin, Etherium, and other virtual currencies that facilitate transactions outside the institutionalized state and global financial system. The evolution of means of payment and financial systems located outside the realms of state control could have far-reaching consequences, such the mobilizing of funds by terrorist groups and subversive organizations and the funding of terrorist activities; the bypassing of sanctions; secret payments for sensitive and prohibited technologies and materials (such as non-conventional weapons, surface-to-surface missiles, cyber capabilities); undermining of the established

39 "NATO Has Survived Trump, For Now," *Haaretz*, July 15, 2018 [Hebrew].

40 Itay Blumenthal, "GSS Head: This Year We Thwarted Cyber Attacks from around the World," *Ynet*, January 30, 2018, https://www.ynet.co.il/articles/0,7340,L-5078254,00.html [Hebrew].

41 http://www.fatf-gafi.org/home.

financial system; impairment of tax collection; cybercrimes and ransom; money laundering; the payment of bribes; and damage to public funds. Different countries take various approaches toward these currencies, but the international system has yet to make a joint decision on the issue. The heads of the financial system in the West do not regard virtual currency as an imminent threat, given the phenomenon's limited scope in comparison to the world capital market. If the phenomenon of digital currencies spreads, it will be necessary to take legislative and enforcement measures on the state level and to reach international agreements that may ultimately be significant to solving the problem.[42]

The need for global cooperation in cyber defense is clear. The International Telecommunications Union is working to promote global agreement regarding defense of the cybersphere. There have also been attempts to formulate an international convention regarding cyber defense, similar to those conventions limiting the proliferation of chemical and biological weapons. The chances are low, however, as it would require reliable oversight and a validation mechanism, which is difficult to implement in the cybersphere.[43] The United States apparently is also concerned that such a convention would limit its abilities and not significantly contribute to its defense, which further decreases the chance of achieving agreement on an effective convention in this realm.

Conclusion

The first part of this article presented the concept of broad economic warfare, which has a wider scope than economic warfare according to the standard definition. The second part of the article discussed cyber warfare as an element of broad economic warfare. Broad economic warfare enables a systemic discussion of a variety of actions that can be conducted against an enemy's economy using diverse tools, including economic, diplomatic, cognitive, kinetic, and cyber means. The aim of these actions is to weaken the enemy's economy, primarily in order to achieve political and military goals. Conducting broad economic warfare in the cyber era depends upon

42 Shmuel Even, "Internet Currencies and National Security," *INSS Insight*, no. 1003, December 28, 2017.

43 Cameron S. Brown and David Friedman, "A Cyber Warfare Convention? Lessons from the Conventions on Chemical and Biological Weapons," in *Arms Control and National Security: New Horizons*, Memorandum no. 135, ed. Emily B. Landau and Anat Kurz (Tel Aviv: Institute for National Security Studies, 2014).

the development of offensive and defensive capabilities alike. Offensive abilities are imperative for the sake of defense, deterrence, and retaliation, whereas defensive cyber capabilities are also essential in offensive situations, in order to withstand a counterattack.

The cyber era has changed the realm of broad economic warfare. From an offensive perspective, it is possible to strike at the enemy's economy during wartime and between wars, using "soft" cyber warfare and high-intensity cyberattacks that may be preferable to kinetic attacks, which are frequently accompanied by human casualties. From a defensive perspective, the increasing dependence on the cybersphere intensifies the cyber threats that are posed to state economies and therefore states require significant efforts and heavy investments to defend the economy, in addition to cooperative efforts within the economy, between the private economy and the government, and among states in the global system.

Although extreme scenarios of cyberattacks on state economies have thus far not materialized, the pace of building defenses for the state cyber system must adapt to the rapidly accelerating establishment of the economy within the cybersphere.

How a Comparative View and Mutual Study of National Strategic Intelligence and Competitive Intelligence Can Benefit Each Other

Avner Barnea

National strategic intelligence and competitive intelligence seem to be two different disciplines. Research has focused on the two fields—national strategic intelligence and competitive intelligence—separately, without any attempt to apply lessons and relevant explanations from one field to the other. Looking deeply into these two fields reveals, however, that they have a lot in common. As the methodology of intelligence in both governments and business has hit a glass ceiling, based on the gaps between expectation and execution in both fields, there is a need to recognize what can be done to improve these practices in both areas. One of the options that has emerged from comparing intelligence performance in both fields is the possibility of applying the accumulated experience in the business field to improve the national one, and vice versa. In both government strategic intelligence and in competitive intelligence, the intelligence discipline is a method of the decision-support system. The use of an objective approach is an important way of assisting chief executives in both fields to avoid mistakes during the process of deciding what to do next.

Keywords: National intelligence, strategic intelligence, competitive intelligence, market intelligence, decision making

Dr. Avner Barnea is a research fellow at the National Security Studies Center, University of Haifa.

Introduction

National strategic intelligence and competitive intelligence appear to be two unrelated fields.[1] In recent years, however, academic research in national, competitive, and marketing intelligence has shown that a comparative analysis can be made of the two areas (government and business), revealing possible relationships between them. One particularly interesting topic is the comparison between the intelligence failures in both areas and how they can be prevented and whether these areas can be assisted by the experience gained from the other in order to improve performance.

Strategic surprises with fateful significance are common in the political-security sphere and in the business sphere. The popular 2011 uprising known as the Arab Spring in Egypt, Tunisia, Yemen, and Syria against the governments and rulers of these countries—including the revolutions that led to the fall of Mubarak's regime in Egypt and to the tragic and destructive civil war in Syria—demonstrate the far- reaching consequences of the strategic surprise in the national arena. In the business arena, the strategic surprise of Nokia—the "world's mobile communications leader"—was the advent of Apple's iPhone (2007), which obliterated both Nokia mobile phones and Kodak consumer cameras. It is only natural that those planning a strategic move do all they can to cause the surprise, while those who are charged with thwarting the opponent's strategic moves do their best to prevent the surprise.[2]

For many years, intelligence capabilities have been recognized as a state's basic skills, as decision makers demand quality intelligence upon which they can depend. A proper definition of intelligence is "secret state activity to understand or influence foreign entities."[3] Herman states that covert intelligence is information gathered by special means, and it starts where the media and the overt sources stop.[4]

---

1 According to SCIP (Strategic and Competitive Intelligence Professionals), competitive intelligence is the process of legally and ethically gathering and analyzing information about competitors and the industries in which they operate in order to help an organization make better decisions and reach its goals. See http://www.scip.org/.

2 Avner Barnea, "Failures in National and Business Intelligence: A Comparative Study," PhD diss. (University of Haifa, School of Social Sciences, 2015).

3 Michael Warner, "Wanted: A Definition of 'Intelligence,'" *Studies in Intelligence* 46, no. 3 (2002):15–22.

4 Michael Herman, "Intelligence and Policy: A comment," *Intelligence and National Security* 6 no. 1 (1991): 229–239.

Since World War II, government decision makers have been aware that intelligence is an important and often critical tool for the national decision-making process. Extensive research of national intelligence began about fifty years ago, and today it is recognized as an integral part of studying international relations and political science.[5]

Competitive and marketing intelligence was introduced and became institutionalized only in the 1980s and even more so since the second half of the 1990s. It was strongly influenced by studying the relevant experience acquired from the national intelligence, together with outstanding inputs from the business sector.[6] Michael Porter's pioneering book *Competitive Strategy*—one of the most influential works in the field of business strategy—was one of the factors that drove the progress of intelligence in business.[7] While the information revolution became significant also in business at the end of the 1990s, the dynamic changes in the competitive environment globally transformed competition and advanced a comprehensive research and academic study in competitive and marketing intelligence.[8]

Early-warning systems are highly recognized both in national intelligence and business intelligence. Looking practically into the implementation of these systems in each field shows that the challenges are quite similar, and

5 Abram Shulsky and Gary Schmitt, *Silent Warfare, Understanding the World of Intelligence* (Washington, DC, Potomac, 2002); Uri Bar-Joseph and Rose McDermott, *Intelligence Success and Failure: The Human Factor* (Oxford: Oxford University Press, 2017); Karin Yarhi-Milo, *Knowing the Adversary: Leaders, Intelligence and Assessment of Intentions in International Relations* (New Haven: Princeton University Press, 2014).

6 Alf H. Walle, *Qualitative Research in Intelligence Marketing: The New Strategic Convergence* (Westport, CT: Quorum Books, 2001).

7 Michael Porter, *Competitive Strategy: Techniques for Analyzing Industries and Competitors* (New York: Free Press, 1980).

8 John Prescott, "The Evolution of Competitive Intelligence, Designing a Process for Action," *APMP* (Spring 1999); Qui Tianjiao, "Scanning for Competitive Intelligence: The Managerial Perspective," *European Journal of Marketing* 42, no. 7/8 (2008): 814–835; Richard G. Vedder, and Stephen S. Guynes, "A Study of Competitive Intelligence Practices in Organizations," *Journal of Computer Information Systems* 41, no. 2 (2000): 36–39; Paul Dishman and Jonathan Calof, "Competitive Intelligence: A Multiphasic Precedent to Market Strategy," *European Journal of Marketing* 42, no. 7/8 (2008): 766–786; Sheila Wright and Jonathan Calof, "The Quest for Competitive, Business and Marketing Intelligence: A Country Comparison of Current Practices," *European Journal of Marketing* 40, no. 5/6 (2006): 453–465.

often they depend upon the interpretation of the intelligence and the interface with the decision makers.[9]

Similarities Between the Two Intelligence Disciplines

The basic assumption in this paper is that in both fields, national and business, the intelligence about the changes in the external environment by rivals or competitors supports the decision-making process. In both fields, there is a need to improve. This could be achieved through cross-functional studies, especially as the decision makers who process the information point to common biases and errors by individuals, which to a greater degree is better researched in business than in intelligence organizations.[10] Based on the review of existing literature on both competitive intelligence and government (strategic) intelligence, this study will look at the perspective of what each field can learn from the other. This study may show that mutual learning will improve the quality of intelligence in order to better understand complicated situations and thus support the decision-making process. This study may be beneficial specifically in avoiding strategic surprises as well as in improving the understanding of complicated situations.

9 Jami Miscik, "Intelligence and the Presidency, How to Get it Right," *Foreign Affairs* (May/June 2017); Ben Gilad, *Early Warning: Using Competitive Intelligence to Anticipate Market Shifts, Control Risk and Create Powerful Strategies* (New York: Amacom, 2004); Cynthia M. Grabo, *Anticipating Surprise: Analysis for Strategic Warning* (University Press of America, 2004).

10 Andrew P. Sage, "Human Judgment and Decision Rules," in *Concise Encyclopedia of Information Processing in Systems and Organizations*, ed. Andrew P. Sage (New York: Pergamon Press, 1990), pp. 227–229; Daniel Kahneman and Amos Tversky, "Choices, Values, and Frames," *American Psychologist* 39 (1984): 341–350; Lowell W. Busenitz and Jay B. Barney, "Differences between Entrepreneurs and Managers in Large Organizations: Biases and Heuristics in Strategic Decision-Making," *Journal of Business Venturing* 12, no. 1 (January 1997): 9–30.

Both disciplines—national intelligence and competitive intelligence—are based on the "intelligence cycle." [11] This cycle is a systematic process of five steps ensuring that intelligence activities are carried out under checks and balances:

1. Definition of key intelligence topics: What we know about the issue and what we need to find out;
2. Collection: Collecting information from several of sources;
3. Organization: Taking all relevant information that has been collected, putting it together, and organizing it;
4. Analysis: Examining all the relevant information that has been collected and determining how it fits together, its meaning, and significance;
5. Processing and distribution: Giving the final analysis to decision makers. The intelligence cycle is a closed loop; feedback must be received from the decision makers, and revised intelligence requirements must be issued.

The similarity between the explanations of intelligence failures in both national and business fields is present in five major areas:

1. Gathering ability: Usually there is no shortage of information;
2. Noisy information environment: Struggles with receiving and classifying information, even prior to the estimation stage, due to large amounts of unclear and sometimes contradicting information;
3. Human factor failures: The literature focuses on the failures of the intelligence analyst and not on the failure to identify the intelligence targets (the other side—the appraised rival, which is the focus of attention of the scattered surprise. Less attention is given to developing an analytic ability to prevent a scattered surprise given the lack of awareness of this matter;
4. Organizational difficulties and deficient cooperation: Failures that are derived from the structural complexity of organizations and inter and intra organizational competitiveness harm cooperation and do not lead to fully utilizing the intelligence;

---

11 Judith Johnston and Rob Johnston, "Testing the Intelligence Cycle Through Systems Modeling and Simulation," in *Analytic Culture in the US Intelligence Community*, ed. Rob Johnston (Washington DC: CIA, Center for the Study of Intelligence, 2005), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/analytic-culture-in-the-u-s-intelligence-community/chapter_4_systems_model.htm; Thomas Smith, *Encyclopedia of the Central Intelligence Agency* (New York: Infobase Publishing, 2003), pp. 137–138; David Omand, *Securing the State* (C. Hurst & Co Publishers, 2010), p. 113–137.

5. Interaction between intelligence and decision makers: This might cause biased estimations and could prevent their transmission, in order to prevent a conflict between the desired policy and the intelligence estimations.[12]

Competitive intelligence has adopted the discipline of national intelligence and applies it to its needs, with necessary modifications. The lack of resources allocated to fulfill the competitive intelligence needs of corporations makes its scope limited, and therefore, the competitive intelligence can deal simultaneously with only a small number of KITs (key intelligence topics) and thus can process less information. However, from its very beginning, competitive intelligence did not focus only on tracking threats from competitors or monitoring significant technological developments (such as digital media replacing the DVD and CD; laser printer replacing the ink-jet printer; digital photography replacing chemical film; and plastics replacing metals and glass, and so forth). It also studied trends in markets, with an emphasis on understanding the customer's desires to make decisions leading to competitive advantage.[13] Competitive intelligence and market intelligence are actually complimentary; competitive intelligence usually monitors broad perspectives of the external environment that may affect corporations, with a deeper view to the future,[14] while market intelligence is focused on the current situation in the markets.[15]

One notable similarity between national intelligence and competitive intelligence is the ongoing attempt to get decision makers to acquire the most from the intelligence presented to them. Monitoring frequent changes in the two areas of business and state security is not easy because it is difficult to assess the significance of signals and noises and to predict the future and thus reduce uncertainty.[16]Another similarity is that in both areas, intelligence is proactive and strives to obtain information that can be alert to the changes

12 Barnea, "Failures in National and Business Intelligence."

13 Jan Herring, "Key Intelligence Topics: A Process to Identify and Define Intelligence Needs," *Competitive Intelligence Review* 10, no. 2 (1999): 4–14.

14 Bernard J. Jaworski, Deborah J. Macinnis, and Ajayk Kohli, "Generating Competitive Intelligence in Organizations," *Journal of Market-Focused Management* 5 (2002): 279–307.

15 Dishman and Calof, "Competitive Intelligence"; Avner Barnea, "Competitive Intelligence in the Defense Industry: A Perspective from Israel – A Case Study Analysis," *Journal of Intelligence Studies in Business* 4, no. 2 (2014): 91–111.

16 Farshad Rafii and Paul J. Kampas, "How to Identify Your Enemies Before They Destroy You," *Harvard Business Review* (November 2002).

in the external environment and their meanings.[17] In both areas, often the intelligence presented to decision makers can be a catalyst for further actions and new initiative to secure advantages.[18]

Competitive intelligence and national intelligence usually deal simultaneously with both tactical and strategic areas to answer different needs and requirements by intelligence consumers; however, senior decision makers tend to seek primarily strategic intelligence.[19] In competitive intelligence, they often work closely with strategic planning units and marketing whereas in national strategic intelligence, these units operate closely and often directly with the senior decision makers,[20] trying to influence and make their inputs recognized.[21]

Positioning Intelligence in the Business Sector

In recent years, we have seen a growing recognition in the business field that competitive intelligence is one of the core competencies required for the decision-making process,[22] like other capabilities, such as marketing, sales, research and development, operations, and human resources. Until the mid-1990s, it was not obvious that a need for competitive intelligence existed. Executives previously achieved their positions in the business world by relying on unorganized information, "gut feelings," and personal experience.[23]

Competitive intelligence has not yet become widely established and still does not occupy its proper place in the minds of the decision makers. For many years, competitive intelligence professionals focused mainly on the

17 Prescott, "The Evolution of Competitive Intelligence."

18 Anders Johansson, Daniel Roos, and Volker Kirchgeorg, "The Art of Systematic Surveillance," *Arthur D. Little* (March 2013), http://www.adlittle.cn/sites/default/files/viewpoints/ADL_Intelligence_management_2012.pdf.

19 Jan Herring, "Senior Management Must Champion Business Intelligence Program," *Journal of Business Strategy* (September–October, 1990): 48–52; Douglas Bernhardt, "Strategic Intelligence for Executives," *Wits Business School Journal* 3, no. 22 (2010).

20 Klaus S. Søilen, "A Place for Intelligence Studies as a Scientific Discipline," *Journal of Intelligence Studies in Business* 5, no. 3 (2015): 35–46.

21 Stephen Marrin, "Why Strategic Intelligence Analysis has Limited Influence on American Foreign Policy," *Intelligence and National Security* 32, no. 6 (2017), http://dx.doi.org/10.1080/02684527.2016.1275139.

22 Robert M. Grant, *Contemporary Strategy Analysis* (Wiley-Blackwell, 2005).

23 Michael D. Watkins and Max H. Bazerman, "Predictable Surprises: The Disaster You Should Have Seen Coming," *Harvard Business Review* (April 1, 2003).

tactical: the immediate actions by competitors and other players, finding out their short-term intentions and identifying changes in the business environment. In recent years, it is possible to see increasing recognition of the comparative advantage of competitive intelligence in the strategic area,[24] supporting the need to recognize and thus assess what is happening around and to know who a company is fighting[25] and contribute to the planning and preparations for the coming years.[26] Søilen showed that while competitive intelligence and market intelligence function is important, the top management can become the problem when a company is struggling to compete, and it can affect the intelligence.[27]

What is Challenging Intelligence?

In national intelligence, as in business intelligence, collection efforts can usually obtain sufficient and significant information that is useful to assess threats and opportunities and their meaning. Intelligence in business, unlike national intelligence that obtains secret information by using large and unique resources, is very careful to follow the law, and its value to business success gets a great degree of recognition.[28] Its activity is based on gathering mainly from public information (known as Open Source Intelligence or OSINT) in a narrower scope, but it is still capable of achieving high-quality results by helping to create a valid intelligence picture of the dynamics of the external environment.[29] Still, competitive intelligence is evolving as the needs of businesses—and not the method or technology supporting the gathering

24 Craig Fleisher, Sheila Wright, and Helen T. Allard, "The Role of Insight Teams in Integrating Diverse Marketing Information Management Techniques," *European Journal of Marketing* 42, no. 7/8 (2008): 836–851.

25 Yuval Atsmon, "To Develop a Winning Strategy, Know Who You Are Fighting," *McKinsey & Company*, June 27, 2017, http://bit.ly/2IB2kZN.

26 John Prescott and Stephen Miller, *Proven Strategies in Competitive Intelligence: Lessons from the Trenches* (New York: Wiley & Sons, 2001).

27 Klaus S. Søilen, "Why Care about Competitive Intelligence and Market Intelligence? The Case of Ericsson and the Swedish Cellulose Company," *Journal of Intelligence Studies in Business* 7, no. 2 (2017): 27–39, https://ojs.hh.se/index.php/JISIB/article/view.

28 Cynthia A. Bulley, Kofi F. Baku, and Michael M. Allan, "Competitive Intelligence Information: A Key Business Success Factor," *Journal of Management and Sustainability* 4, no. 2 (2014).

29 Leonard M. Fuld, *The Secret Language of Competitive Intelligence* (New York: Crown Business, 2007).

and analysis of information—change.[30] In business, it is preferred to have a single organization unit that is responsible for intelligence and strategy but at the same time to include cross-functional teams to support the analysis of information.[31] What really matters more than the type and quantity of the data is establishing a deep corporate culture of evidence-based decision-making. According to O'Connell and Frick, it also means encouraging everyone in the organization to use data more effectively.[32]

Competitive and market intelligence were pioneers in developing significant capabilities in monitoring social media and using the insights obtained as an additional tool in the process of making decisions.[33] Real-time social media information as well as traditional market and competitive intelligence provide detailed pictures and tell a comprehensive story than neither alone can deliver. Big data accelerates these capabilities. This formula was recently presented by the leading business consulting firm, McKinsey. In this important article, the authors stated that the business world had developed advanced analytical tools for obtaining vast business information extracted from social media in addition to "conventional" sources.[34] National intelligence also gives increased weight to OSINT, revealed as important and qualitative, which

30 John McGonagle and Michael Misner-Elias, "The Changing Landscape of Competitive Intelligence: Two Critical Issues Investigated," *Salus Journal* 4, no. 1 (2016); Troy Mouton, "Organizational Culture's Contributions to Security Failures," MA thesis (Louisiana State University, 2002), http://digitalcommons.lsu.edu/cgi/viewcontent.cgi?article=2120&context=gradschool_theses; Ming-Jer Chen and Mary Summers Whittle, "Competitor Acumen: The Heart of Competitor Analysis," Darden Case No. UVA-S-0293, https://ssrn.com/abstract=2975253; Nanette J. Bulger, "The Evolving Role of Intelligence: Migrating from Traditional Competitive Intelligence to Integrated Intelligence," *International Journal of Intelligence, Security and Public Affairs* 18, no. 1 (2016): 57–84.

31 Gary L. Neilson, Karla L. Martin, and Elizabeth Powers, "The Secrets to Successful Strategy Execution," *Harvard Business Review* (June 2008).

32 Andrew O'Connell and Walter Frick, "You Have Got the Information, but What Does it Mean? Welcome to 'From Data to Action,'" *Harvard Business Review*, (November 19, 2013).

33 Fleisher, Wright and Allard, "The Role of Insight Teams in Integrating Diverse Marketing Information Management Techniques," *European Journal of Marketing* 42 no. 7/8 (2008): 836–851; Topi Laakso, *Handbook of Social Media Intelligence*, *(*M-Brain, 2016).

34 Martin Harrysson, Estelle Métayer, and Hugo Sarrazin, "How 'Social Intelligence' Can Guide Decisions," *McKinsey Quarterly* (November 2012).

can hardly be ignored. If in the past, one could argue that national strategic intelligence relied primarily on secret information, it is now changing fast. OSINT has become highly significant as we are living in an age of growing transparency.[35] In recent years, social media has become a significant source of national intelligence,[36] while it already has been a source for competitive and marketing intelligence for over the past ten years.[37]

With the fast development of the internet, the information revolution, and more recently, the enormous growth of social media, the business world has become much more transparent than in the past. Difficulties in getting important information have gradually declined, but the main problem remains in how to deal with vast amounts of information. The utmost challenge is the development of analytical capabilities that can benefit from the information obtained. A new evolution of social competitive intelligence has emerged, meaning that competitive intelligence is better performed in a networking organization that supports the analytical process.[38]

The American intelligence community is gradually granting higher priority to the value of OSINT. Since the Arab Spring, US intelligence has recognized the need to understand trends, preferences, and perceptions among wider audiences, where the business world is already well experienced through research and marketing intelligence that monitors massive crowds

35 Sean P. Larkin, "The Age of Transparency," *Foreign Affairs*, 95, no. 3 (May/June 2016): 136–146; Nicholas Ballasy, "Brennan: CIA Must Rely on Social Media in the Middle East," *PJ Media* (May 20, 2015), http://pjmedia.com/blog/brennan-cia-must-rely-on-social-media-in-the-middle-east/.

36 Eyal Pascovich, "Intelligence Assessment Regarding Social Developments: The Israeli Experience," *International Journal of Intelligence and CounterIntelligence* 26, no. 1 (2013): 84–114; Kristan J. Wheaton and Melonie Richey, "The Potential of Social Networks in Intelligence," *E-International Relations* (January 9, 2014), http://www.e-ir.info/2014/01/09/the-potential-of-social-network-analysis-in-intelligence/.

37 Lars Degerstedt, "Social Competitive Intelligence: Socio-Technical Themes and Values for the Networking Organization," *Journal of Intelligence Studies in Business* 5, no. 3 (2015): 5–34.

38 Ibid.

of customers. Other western intelligence communities, including Israel,[39] follow comparable directions, drawing similar lessons from the Arab Spring.[40]

In business, one of the most significant capabilities of qualitative collection is through the employees themselves. Since many of them have wide contacts with parties outside their company as part of their duties, they are exposed to important information that can help achieve a competitive advantage. This requires competitive intelligence professionals to build internal networks often through informal relationships with relevant employees and brief them on KITs and get from them information that comes to their attention. Note that business firms are strict on keeping their activities legal and are careful to work according to codes of ethics. In recent years, with the rapid development of OSINT and particularly social media, many companies maintain contacts with their employees through internal social media systems and other applications to share useful competitive information.[41]

It appears that corporations are longing to be in the position as described by Cisco's CEO John Chambers: "We understand the market, our competitors and—most importantly—how our competitors think . . . I have a pretty good idea what their next two moves will be."[42]

Intelligence Failures in National and Business Intelligence

One of the definitions of intelligence failure is taken from the CIA: "Systemic organizational surprise resulting from incorrect, missing, discarded, or inadequate hypotheses." According to another definition, intelligence failure is "organizational surprise resulting from incorrect information, a lack of

39 Pascovich, "Intelligence Assessment Regarding Social Developments."

40 CIA, "INTellingence: Open Source Intelligence," *CIA: News and Information,* (2010), https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html.

41 Maral Mayeh, Rens Scheepers, and Michael Valos, "Understanding the Role of Social Media Monitoring in Generating External Intelligence," Twenty-third Australasian Conference on Information Systems*,* Geelong (December 3–5, 2012).

42 John Swartz, "Cisco's Chambers: 2 Days with Man on a Mission at CES," *USA Today* (January 9, 2013), http://www.usatoday.com/story/tech/2013/01/09/cisco-ibm-oracle-hp/1791255/.

information, from neglect or inadequate hypotheses."[43] Often it means late detection of a significant threat that gives a substantial advantage to the initiator side, resulting in significant damage to the other side.[44] Examining the failures and the reasons for their occurrence leads to the conclusion that it was possible to prevent them in many cases.[45] The reasons for failures usually do not arise from a lack of information but rather from the human factor; that is, misunderstanding the meanings of available information and poor evaluation of new and unfamiliar threats.[46] The result is an incorrect presentation of the threat's meaning, organizational failures, and difficulties in the application of the "intelligence culture."[47] Too often this is also a result of the diffusion of political considerations into intelligence assessments,[48] which is apparent in the "Report on the US Intelligence Community's Prewar Intelligence Assessment on Iraq" from 2004.[49] When heads of states refrain from intelligence warnings, it is not considered an intelligence failure.[50]

One of the leading and greatest scholars within the field of military and security strategy, Yehoshafat Harkabi from Israel, emphasized that the lack of distinction between threats is a result of cognitive failures causing difficulties

43 Rob Johnston, *Analytic Culture in the US Intelligence Community: An Ethnographic Study* (Central Intelligence Agency, 2005), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/analytic-culture-in-the-u-s-intelligence-community/chapter_1.htm.

44 Bar-Joseph and McDermott, *Intelligence Success and Failure: The Human Factor*, pp. 13–17.

45 Paul R. Pillar, "Presidents Make Decisions Based on Intelligence," *Foreign Policy* (Jan/Feb 2012).

46 Bar-Joseph and McDermott, *Intelligence Success and Failure: The Human Factor*, pp. 13–17.

47 Philip Davies, "Intelligence Culture and Intelligence Failure in Britain and the United States," *Cambridge Review of International Affairs* 17, no. 3 (October 2004): 495–520; Mouton, "Organizational Culture's Contributions to Security Failures."

48 Zeev Maoz, "Intelligence Failures: An Analytical Framework," paper presented at the annual meeting of the American Political Science Association, Philadelphia, PA, August 31, 2006, http://www.allacademic.com/meta/p151465_index.html.

49 Russ Travers, "The Coming Intelligence Failure: *A Blueprint For Survival*," *Studies in Intelligence*, no. 1 (1997), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/97unclass/failure.html.

50 Mark A. Jensen, "Intelligence Failures: What Are They Really and What Do We Do about Them?" *Intelligence and National Security* 27, no. 2 (2012): 261–282.

to produce a realistic picture.[51] After failures of strategic intelligence at the national level, usually governments conduct a comprehensive examination into the causes of the failures, in order to avoid them in the future and to expose their results to the public (such as the 9/11 Commission Report, 2004). In most surprise attacks since 1939, intelligence communities claimed beforehand that an attack was not imminent so decision makers later pointed the finger at intelligence for not foreseeing the attack.[52] Expectations of improving the quality of intelligence with the increase of resources and tools in recent years did not materialize, and the capabilities of the American, British, and Israeli intelligence did not show significant improvements while the reasons for failures remained the same.[53]

Business intelligence failure can be defined as a significant surprise caused by an erroneous assessment of the competitive environment.[54] Unfortunately comprehensive review processes and lessons learned from business failures are less common.[55] However, in recent years it has been recognized that some of the reasons for business failures also lie in the lack of intelligence processes, difficulties with managers to identify changes in the business environment, biased information submitted, their intent to be appeased, or decision makers who ignored intelligence presented to them. This is precisely what happened to Nortel, a world leader in telecommunications, when the senior management ignored early-warning signals about major changes in the competitive environment provided by its competitive intelligence unit;[56] this was one of the key factors that led to its collapse.[57] Furthermore, as

51 Yehoshafat Harkabi, *Fundamentals in the Israeli Arab Conflict* (Tel Aviv: Ministry of Defense Publishing, 1971) [Hebrew].

52 Bar-Joseph and McDermott, *Intelligence Success and Failure*, pp. 17–19.

53 Richard Betts, "Fixing Intelligence," *Foreign Affairs* 81(2002): 43–59.

54 Natalia Tsitoura and Derek Stephens, "Development and Evaluation of a Framework to Explain Causes of Competitive Intelligence Failures," *Information Research* 17, no. 2 (June 2012).

55 Avner Barnea, "Lack of Peripheral Vision – How Starbucks Failed in Israel?" *African Journal of Marketing Management* 3, no. 4 (April 2011): 78–88.

56 Paul Schoemaker, George S. Day, and Scott A. Snyder, "Integrating Organizational Networks, Weak Signals, Strategic Radars and Scenario Planning," *Technological Forecasting and Social Change* 80 no. 4 (2013): 815–824.

57 Jonathan Calof, Laurent Mirabeau, and Greg Richards, "Towards an Environmental Awareness Model Integrating Formal and Informal Mechanisms – Lessons Learned from the Demise of Nortel," *Journal of Intelligence Studies in Business* 5, no. 1 (2015): 57–69.

a result of the size of corporations, pockets of quality intelligence are available for individuals or small groups that do not impede formulating the intelligence picture.[58] The outcome is often the lack of submission of important information to the decision makers, usually as a result of an absence of intelligence awareness or a voluntarily tendency to preserve power without sharing information.

The business sector is gradually moving toward internal sharing of information and has concluded that information sharing, especially about the external environment, is one of the means to strengthen business competitiveness.[59] The belief is that quality information already exists internally and has to be channeled to support decisions. In national intelligence, sharing information is one of the most important lessons learned from the Inquiry Commission of the 9/11 terrorist attack. The implementation of sharing information in national intelligence encountered difficulties and had internal opposition due to a disproportionate amount of secrecy and compartmentalization, resulting from limited vision and fixation of thought.[60] In the opinion of the 9/11 Inquiry Commission, this was one of the major reasons that caused the intelligence failure that could have prevented the 9/11 terrorist attacks.[61] We also saw this problem in the failure to prevent the terrorist attack at the Boston Marathon in April 2013.[62]

Following the 9/11 attacks and the subsequent failure to properly assess Iraq's Weapons of Mass Destruction program in 2003—two intelligence

58 Kurt April and Julian Bessa, "A Critique of the Strategic Competitive Intelligence Process within a Global Energy Multinational," Problems and Perspectives in Management 4, no. 2 (2006), https://businessperspectives.org/journals/problems-and-perspectives-in-management/issue-10/a-critique-of-the-strategic-competitive-intelligence-process-within-a-global-energy-multinational.

59 Christopher G. Myers, "Is Your Company Encouraging Employees to Share What They Know?" *Harvard Business Review* (November 6, 2015); Clayton Christensen, "Knowledge Sharing: Moving Away from the Obsession with Best Practices," *Journal of Knowledge Management* 11, no. 1 (2007): 36–47.

60 Gregory Treverton, *Intelligence for an Age of Terror* (New York: Cambridge University Press, 2009), pp. 1–14.

61 "The 9/11 Commission Report," (2004), http://www.911commission.gov/report/911Report.pdf.

62 Mark Giuliano, "How the FBI is Evolving to Meet Threats in a Changing Environment," *From the Boston Marathon to the Islamic State, Stein Counterterrorism Lectures,* ed. Matthew Levitt, Counterterrorism Lecture 6 Policy Focus 139 (Washington DC: The Washington Institute for Near East Policy, 2014), pp. 9–16.

failures exhibiting two completely different types of errors[63]—official investigations were conducted to determine their underlying causes. No consideration was given to the potential inputs from the analytical models used in the business sector. All recommendations were to do more of the same inside the national intelligence practices. After oversights in analysis that culminated in the failure to warn of the fall of the Berlin Wall (1989) and the subsequent collapse of the Soviet Union, the US intelligence community also had reached similar conclusions years before to do minor changes, which actually did not improve the quality of analysis. No serious consideration was given to explore outside the box of already known analytical practices used by the business community and the academy.

Academic research of business failures does not often highlight failures of intelligence but rather studies other causes, such as unsuitable products, inadequate pricing, slow reaction to the competition, wrong strategic moves, and personal management mistakes of executives.[64] In numerous cases, especially in large corporations where the price of failure is high, the failure could be repaired in a reasonable time and therefore is less alarming compared to similar consequences of national intelligence failures. Some of the most serious threats to firms might not even be perceived as such.[65] Acceptable solutions for business failures, such as replacing senior management and organizational changes, usually ignore a lack of intelligence or deficient attention by the decision makers. A compelling example is the business failure by Levi's[66] and Nokia.[67]

Around the world, including Israel, it seems that the number of directors who understand that quality and timely intelligence is critical to business success is increasing and therefore implementing the discipline of competitive and market intelligence into their organizations has become common practice.

---

63 Richard Betts, "Two Faces of Intelligence Failure: September 11 and Iraq's missing WMD," *Political Science Quarterly* 122, no. 4 (2007): 585–606.

64 Kevin Coyene and John Horn, "Predicting you Competitor's Reactions," *Harvard Business Review* (April 2009).

65 Michael Stahl and David Grigsby, *Strategic Management for Decision Making* (New York: KWS Kent Publishing, 1992).

66 Mathew Olson, Derek van Bever, and Seth Verry, "When Growth Stalls," *Harvard Business Review* (March 2008).

67 James Surowiecki, "Where Nokia Went Wrong?" *New Yorker* (September 13, 2013), http://www.newyorker.com/online/blogs/currency/2013/09/where-nokia-went-wrong.html?printable=true&currentPage=all.

What Can National Intelligence Learn from Competitive and Market Intelligence?

For years, conventional business thinking recognized that competitive and market intelligence studies come from the experience of national intelligence[68] in several fields:

1. Implementing "the intelligence cycle" into the business intelligence process
2. Focusing the intelligence methodology in the firm around KITs
3. Setting up closed interaction between intelligence and decision makers, using intelligence indicators for warning of threats in the competitive environment, such as loss of market share, difficulties with major customers, decreased interest in competitors by the senior management, ignoring new competitors, delays in response to changes, and lack of knowledge about competitors.

The challenge is to implement a new cross-organizational discipline, which often faces firm objections and resistance to change.[69] This challenge was the focal point of the paper about implementing competitive intelligence in organizations by Arthur D. Little's consultancy, "The Art of Systematic Surveillance."[70]

The US intelligence community mistakenly thought that it could not learn from experience gained by business intelligence despite the fact that the intelligence committees of the US Congress and a few experts within the community tried to convince them that this approach was wrong. It turns out that national intelligence previously tested rival organizations based on confidential information and usually ignored OSINT.[71] They neglected to analyze large audiences, for example, for early recognition of civil unrest or changing trends among audiences threatening the existing regimes. Meanwhile, the business world had acquired vast and successful experience using marketing research and collecting public information to identify consumer preferences and analyze competitors moves. David Shedd, deputy director of the Defense Intelligence Agency, noted the recent failure of intelligence in predicting the events of the Arab Spring: "Analysts failed

68 Thomas Kelley, *Marketing Intelligence: The Management of Marketing Information* (London: Staples Press, 1968).

69 Søilen, "Why Care about Competitive Intelligence and Market Intelligence?"

70 Johansson, Roos, and Kirchgeorg, "The Art of Systematic Surveillance."

71 David Steele, "The Open Source Program: Missing in Action," *International Journal of Intelligence and CounterIntelligence* 21 no. 3 (2008): 609–619.

to note signs that would have indicated to us, shown us, that there was a growing dissatisfaction . . . in the general population. We missed that."[72] These events led the US intelligence agencies to examine relevant business experience, analyzing the positions of broad audiences (crowd sourcing) in conjunction with academia and many global companies, including Intel, HP, Dell, Google, Eli Lilly, Procter & Gamble, and General Electric.

An additional field that allows American intelligence to learn from these business experiences is in forecasting markets,[73] known as prediction markets. This extensive business experience allows us to estimate the directions and trends in the markets and get early warnings of possible significant changes.[74] Intelligence communities in the United States and Israel have looked recently toward the experience acquired by the business' sector in measuring performance and specifically, the value of information.[75]

---

72 Ken Dilanian, "U.S. Intelligence Official Acknowledges Missed Arab Spring Signs," *Los Angeles Times*, July 19, 2012, http://latimesblogs.latimes.com/world_now/2012/07/us-intelligence-official-acknowledges-missed-signs-ahead-of-arab-spring-.html. In the case of the uprising against the Shah in Iran in 1979, the US intelligence community missed the indicators regarding the coming uprising of the population against the regime. See Douglas MacEachin and Janne E. Nolan, "Iran: Intelligence Failure or Policy Stalemate?" in *Discourse, Dissent, and Strategic Surprise Formulating U.S. Security Policy in an Age of Uncertainty*, ed. Douglas MacEachin and Janne E. Nolan (Washington DC: Institute for the Study of Diplomacy, Georgetown University, 2006).

73 Richard Betts, "Analysis, War and Decision: Why Intelligence Failures Are Inevitable?" *Strategic Intelligence: Windows into a Secret World, an Anthology*, ed. Loch Johnson and James Wirtz (Los Angeles: Roxbury Publishing, 2004), pp. 97–99.

74 Poung Fei Yeh, "Using Prediction Markets to Enhance US Intelligence Capabilities," *Studies in Intelligence* 50, no. 4 (2006).

75 Boyd Hendriks and Ian Wooler, "Establishing the return on investment for information and knowledge services," *Business Information Review* 23, no. 1 (2006): 13–25; John Hollister Hedley, "Learning from Intelligence Failures," *International Journal of Intelligence and CounterIntelligence* 18, no. 3 (Fall 2005): 435–450; Asaf Gilad and Meir Orbach, "8200 Silicon Valley Corner: The IDF's Largest Unit is Learning to Work like a Start-up," *Calcalist* (July 1, 2012) [Hebrew], http://www.calcalist.co.il/internet/articles/0,7340,L-3575727,00.html; David Moore, Lisa Krizan, and Elizabeth Moore, "Evaluating Intelligence: A Competency-Based Model," *International Journal of Intelligence and CounterIntelligence* 18, no. 2, (Summer 2005): 204–220.

The Interrelations Between National Intelligence and Competitive Intelligence: A Case Study[76]

Often large corporations find it difficult to forecast future events and threats in the competitive arena, even though there are particularly good tools to improve business forecasting, such as the Four Corners Model by Porter[77] and proven models that have been offered by Jack Welch, the former CEO of General Electric.[78] These competitive failures can cause unexpected difficulties that may lead to a corporation's collapse and, in extreme cases, to bankruptcy. However, these business failures are not unusual incidents, and they occur time and again. It is actually one of the responsibilities of competitive intelligence directors to present industry forecasts to the decision makers and also to the board of directors.

Zim Ltd. was a leading Israeli corporation in the shipping business, among the ten largest in the global industry of marine containers.[79] In 2009, Zim made a presentation to its bond holders, in preparation for a discussion about possibly deploying its debt. The presentation, which included graphs, showed the predicted increase in the volume of maritime transport versus the investments in building new ships expected in the coming years. The shipbuilding business has no secrets: The number of ships being built and requested delivery dates are public information. No one builds ship containers in their backyards and takes them secretly into the sea. It was possible to see that the production rate of ships was growing faster than the projected rate of cargo. According to that presentation, the capacity of marine transportation was to increase by three and a half times, from 4.9 million TEU (unit of measurement accepted in containers) in the year 2000 to 17.9 million TEU by the year 2013. The world's trade was not expected to increase at a similar rate in these thirteen years, hence creating a surplus capacity of shipping containers. Moreover, since late 2008, the situation had become worse as the demand had decreased, which dramatically exacerbated the problem of over capacity in shipping transport.

---

76 Nathan Sheva, "Zim lost 186 million $," *Marker* (August 27, 2009) [Hebrew], http://www.themarker.com/tmc/article.jhtml?ElementId=nl20090827_78683; Doron Zur, "Sail with the Herd," *Marker* (August 23, 2009) [Hebrew].

77 Porter, *Competitive Strategy.*

78 Jack Welch, *Winning* (New York: Harpers Business, 2005).

79 This case study about Zim Ltd is presented briefly, while the aspects of the intelligence failure have been given special attention.

However, even without this decline in the demand for shipping capacity, there was still over capacity as a result of too many ships that were being built. If Zim could see the surplus capacity expected for sea transport, why did it enter into a strategic plan of acquiring massive ships and entering into a huge debt, a plan that could endanger its very existence?

Zim's annual report from 2004 by its parent company, the Israel Corporation Ltd., had predicted the following based on intelligence reports: "The management of Zim ships mentioned that the supply growth rate is expected to be higher than the growth in demand for transport of containers, given the increase in new orders for ships under construction. Such growth could have a significant impact on the business results of the leading marine companies." If this situation was evident already in 2004 —too much supply of transport capacity—and this same statement appeared in the management reviews, showing that the senior management was exposed to this assessment, then the question remains: why did the senior management of Zim decide to enter into a massive investment program in 2006 and 2007 and order new ships?

If a competitive intelligence analyst identifies expected surplus capacity in two or three years, the most logical thing to do would be to advise the senior management to replace the fixed costs with variable costs and reduce debt; that is, it was not worth buying ships and equipment or to make long-term lease agreements. It was better to sell ships, shorten long-term leases, and focus on short-term contracts. In this way, when it was low tide, one could easily reduce costs and return ships whose lease dates had passed. The problem was that life does not always work like this. First, such tactics would hurt profitability in the short term, at the price of increasing the running costs for future flexibility and reducing risk. Second, nobody wants to be the one that diminishes a growing industry. Therefore, management tends to do what everyone else is doing and expand when all are doing so. This was a familiar human weakness and also a cognitive bias: We prefer to be wrong with everyone than to be right alone.

There is a lesson to learn from this case: People working in the business world should be able to disconnect from groupthink. It is easy to say and more difficult to perform. The excess of current production capacity was a heavy burden on Zim's shoulders for several years after 2009, which later led it into bankruptcy.

What are the lessons learned from the competitive intelligence aspects? Was it possible to avoid the catastrophic financial situation that Zim reached in 2009 through the use of competitive intelligence analysis? The answer is clearly yes. Competitive intelligence is also about identifying the big trends that will reshape the business environment and the drivers that disrupt the industry. It is possible to prepare forecasts for various industries, including shipping, mostly as the information is open and accessible. This analysis will help to identify which trends will have the highest impact, what issues disruptions could cause, and what possible future scenarios are suggested.

Table 1. Using intelligence tools to improve the decision-making process

Areas of activity	**Imported tools from competitive intelligence**	**Imported tools from national intelligence (potential)**
Analysis	SWOT	Early-warning indicators
Gathering	OSINT	KITs
Management of uncertainties	Forecasting	Opportunity analysis

Intelligence tools from national strategic and business intelligence could have helped the decision makers and Zim. The use of forecasting, SWOT analysis, and OSINT (Table 1, second column above), was not enough to have a strong impact on the decision makers who ignored this analysis, later bringing Zim to bankruptcy. Zim could have improved its intelligence performance by using tools acquired from the national intelligence discipline (Table 1, third column), such as early-warning indicators, so that Zim would have known better about threats as a result of global changes in international commerce; KITs to improve focus on what was really important for Zim at that stage; and opportunity analysis, which could have identified external opportunities and vulnerabilities that could have been exploited to advance a more careful strategy.[80] An insightful view will never give the answers; however, only concise strategic intelligence efforts could have provided Zim's decision makers with the inconvenient truth of what was really going to happen to Zim if it ignored the drivers of change in the competitive arena.

80 Karen Rothwell, "Opportunity Analysis in an Intelligence Context," *Competitive Intelligence Magazine* 15, no. 1(January/March 2012).

Conclusion

Intelligence failures, including missing the prediction of the Arab Spring, has led the American, British, and Israeli intelligence agencies to examine the accuracy of relevant experiences in business analysis of large audiences, forecasting, opportunity-analysis techniques, and attempts to measure the value of information, all well-known in the business world. National intelligence organizations seem to have gradually comprehended the need to study other disciplines, including the business field, to see how they could enhance their abilities and the necessity of opening up to the business sector and implementing new capabilities, which, after making adjustments, could help confront the challenges they are facing. An excellent example is how the FBI reinvented itself after 9/11 and reorganized itself from a law enforcement agency to a national security organization as a result of a study by three notable scholars from Harvard, led by Jan Rivkin, using specialized academic capabilities in organizational design and organizational identity.[81]

Those engaged in competitive and market intelligence disciplines constantly strive to reach the highest professional level recognized by national intelligence and see there the true model for information and intelligence management. On the other hand, by using intelligence discipline it is possible to create early warnings, even before the burst of a major economic event like the 2008 financial crisis,[82] which changed the economic history of the world. This is also true of many other strong corporations, which failed to see the changes made by competitors and strategic market moves, which left them without any likelihood of surviving.

In both government intelligence and in competitive intelligence, the intelligence discipline is a method of the decision support system. The use of an objective approach is an important way of assisting chief executives in both fields to avoid mistakes in the process of deciding what to do next. It leads to a more careful evaluation of alternatives and dimensions in a comprehensive way, thus overcoming many of the problems associated

81 Ranjay Gulati, Ryan Raffaeli and Jan Rivkin, "Does 'What We Do' Make Us 'Who We Are'? Organizational Design and Identity Change at the Federal Bureau of Investigation," *Harvard Business School* Working Paper 16-084 (January 12, 2016).

82 Timothy Walton, "The 2007–2008 Financial Crisis as a Way to Better Understand Intelligence Failure," paper presented in ISA conference, April 2012; Avner Barnea, "Financial Crisis as an Intelligence Failure," *Competitive Intelligence Magazine* 14, no. 2 (April/June 2011).

with biases in information processing, biases in group dynamics, and in individual decision making. In addition, intelligence analysis has the benefit of displaying all the information in a systematic way for key decision makers.

Cyber, Intelligence, and Security

Call for Papers

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

Articles may relate to the following issues:

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

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

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

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

The Institute for National Security Studies – Cyber Security Program
40, Haim Levanon St, POB 39950, Ramat Aviv, Tel Aviv 61398 | Tel: +972-3-6400400 | Fax: +972-3-7447588