Developing a Doctrine for Cyberwarfare in the Conventional Campaign

Ron Tira

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

Keywords: Cyber, Israel, United States, warfare

Toward the Normalization of State Cyberwarfare

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Characteristics of Cyberwarfare

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

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

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

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

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

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

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

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

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

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

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

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

The Defensive Cyberwarfare Campaign

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

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

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

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

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

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

The Offensive Cyberwarfare Campaign

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

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

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

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

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

Integration of Cyberwarfare in a Conventional Campaign

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

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

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

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

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

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

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

Conclusion: Security Versus a Defensive Campaign

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

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

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

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