2020 12th International Conference on Cyber Conflict
20/20 Vision: The Next Decade
T. Jančárková, L. Lindström,
M. Signoretti, I. Tolga, G. Visky (Eds.)
2020 © NATO CCDCOE Publications, Tallinn

Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations

Matthias Schulze
Associate
International Security Division
German Institute for International and Security Affairs (SWP)
Berlin, Germany

Abstract: The study analyzes the use of cyber capabilities in war and conflict situations. The research question is: What good is cyber in war? What is the utility of military cyber operations in conflict situations and what obstacles exist? The paper analyzes a small set of cases where cyber capabilities have been used for military purposes. Using the 'three levels of warfare' heuristic, the study outlines the potentials and operational restrictions of military cyber operations. The analysis proposes a set of variables and hypotheses, such as the timing of use of cyber capabilities and the operational complexity of a cyber operation, for further theory building.

Keywords: *cyber in war, military cyber operations, levels of war, strategic cyber attacks, tactical cyber, small-n case study*

1. INTRODUCTION

North Korea's leader, Kim Jong-un, allegedly heralded cyber capabilities as an "all-purpose sword" that guarantees "ruthless striking capability" (Young Kong, Gon Kim, and Lim 2019). Popular books, such as *The Perfect Weapon* by David Sanger, frame cyber capabilities as the Swiss Army knife of war, which can be used for all kinds of purposes. Offensive cyber capabilities are often seen as “force multipliers” with high precision, global-reach, relatively low cost and potentially high impact (Smeets 2018b, 98). Strategic cyber warfare conducted by the military to shut down an adversary’s critical infrastructure, a type of “cyber Pearl Harbor,” has been hyped as the next revolution in military affairs, but has not materialized so far (Lawson 2013). Besides deterrence, norms, and taboos, one explanation for this lack of cyber warfare could be the severely limited strategic utility of cyber in war (Libicki 2009, 117). Beyond the strategic level, more and more studies highlight the limitations of cyber operations in conflict situations.

This paper aims to analyze the utility and potential unsuitability of military cyber operations in war or conflict contexts. For that purpose, the study analyzes a small set of cases where cyber operations have been used for military purposes. The paper uses the ‘three levels of warfare’ heuristic, which distinguishes between cyber operations on the strategic, operational, and tactical levels, to sketch out the utility of cyber technology on each of these. This approach is taken because prior research suggests that the strategic utility of cyber is limited (Valeriano, Jensen, and Maness 2018); the same, however, may not be true for the other levels of warfare. The research question thus is: What good is cyber technology in war? What is the utility of military cyber operations in conflict situations and what obstacles exist?

Cyber warfare often lacks the central components of war: large-scale physical destruction, massive violence and compelling an actor to the political will of another (Rid 2012). While the stand-alone use of cyber capabilities might not be regarded as war, the use of *cyber in war* is a feature of almost all modern armed conflicts, from Kosovo 1998 to Ukraine 2014. This study focuses on the use of cyber in war, generally understood as military cyber operations that are defined as a “sequence of coordinated actions with a defined military purpose in cyberspace; requiring cyber capabilities” (van Haaster 2019, 148). The term *operations* indicates a sequential or parallel use of offensive cyber attacks in a coordinated manner, in contrast to singular cyber attacks. The goal of the conduct of war, in general, is not just to destroy or disable physical infrastructures and forces, but to achieve psychological effects, such as compelling an enemy to do one’s will (Clausewitz 1982).

2. TYPES OF CYBER OPERATIONS IN WAR

Cyber in war has the following characteristics. First, cyber attacks in war are often conducted by military organizations, such as cyber commands. Second, these are often, but not exclusively, targeted against opponents’ military infrastructures such as headquarters, command and control, and weapon systems. Cyber attacks in war are often counter-force attacks and stand in contrast to the use of strategic cyber attacks in peacetime to influence the decision calculus of adversaries (Smeets 2018b). Third, they serve a military rather than an intelligence purpose, such as supporting other forces in combat, and thus have a military intention. The distinction between military and non-military cyber operations is, however, not clear-cut. Ambiguities remain because of the attribution problem, as well as the functional overlap with cyber espionage that is conducted by intelligence agencies.

Military theory divides war into three levels: strategic, operational, and tactical. These levels are interrelated and what happens on one level influences the others. The strategic level deals with issues of "how to win a war" (Bateman 2015). The strategic level allocates national resources and instruments of power to achieve victory in war. Strategies ideally define how to use the various means of state power, including cyber capabilities, toward the end of achieving peace. As Clausewitz famously highlighted, the political level of war often cannot be clearly separated from the strategic (Clausewitz 1982). In most democracies, the political level – that is, elected politicians not generals – decide when to go to war.

Strategic attacks, whether kinetic or cyber, are those that try to achieve strategic objectives such as weakening the adversaries' ability or will to engage in conflict (US Air Force 2019). Strategic cyber attacks typically target sources of national power or society in general (Libicki 2009, 117). John Arquilla defines strategic cyber warfare as a "means of striking in very costly, disruptive ways at an adversary without a prior need to defeat opposing military forces in the field, at sea, or in the air" (Arquilla 2017). Strategic cyber attacks are often used as a stand-alone capability that can be executed without mobilizing other, more conventional forces. Cyber attacks in peacetime that target vital functions of a state, such as critical infrastructures, fall into the strategic category, but so do the defend forward or preparation of the battlefield strategies. Strategic cyber attacks are also used for tacit-bargaining, coercion or deterrence (Borghard and Lonergan 2017).

Below the strategic level is the operational level, which is often concerned with the conduct of campaigns and the question of how to employ forces in various theaters, such as a geographic region (Valeriano and Maness 2015, 243). The goal on the operational level is to obtain advantages over the enemy in a series of battles. Targets on the operational level tend to be military, such as enemy ships, tanks or troops, especially if battles take place far from civilian infrastructures. The Allied invasion of Normandy, Operation Overlord, was one operation among many in a specific theater of war to achieve the strategic objective of defeating Nazi Germany. Operational cyber attacks often serve as an "adjunct" function to traditional military forces (Gartzke 2013, 66), that is using the cyber domain together (jointly) with the other domains of warfare (Sanger 2018, 41). For instance, cyber capabilities can be used as a distraction in the early phases of a war to sow confusion and panic on one front, while other forces move in from another direction unobstructed (Jun, LaFoy and Sohn 2015, 15).

Lastly, the tactical level is the realm of combat engagements between individual warfighters and units in a combat situation. Most traditional weapon systems operate at this level. The tactical level thus deals with the conduct and movement of troops in a given terrain. Not much has been written about *tactical cyber*. Cyber operations on the tactical level take place "in the context of a traditional kinetic battlefield, where authorization, deconfliction, and control for the specific operation is at battalion level or lower" (Metcalf and Barber 2014). Deconfliction means overcoming different areas of responsibility of military command levels or between agencies, for example between high-level intelligence agencies and battalion units. An example could be a combat mission, such as a hostage rescue in a "smart city", where video cameras are hacked to provide special forces with situational awareness (Crane and Peeke 2016). IT equipment, drones or GPS devices of combatants could be interfered with using cyber operations. Tactical cyber could take two forms. One is the integration of IT specialists into small units in the field. The second variant is that soldiers can rely on "remote cyber support" from a unit placed somewhere at a safe distance (Porche et al. 2017, 47).

3. CASE STUDIES

This paper uses an inductive or hypothesis-generating case study design that is not based on a full-fledged theory (Levy 2008, 5). Since there is no statistically meaningful number of cases of military cyber operations, the study examines variables in a small number of cases (small-n). The purpose is to develop theoretical propositions about the use of military cyber operations which then can be tested by future research. The aim is to deduce variables that explain the utility of cyber in war. The cases in question are known instances where cyber operations were used in a military context or were conducted by a military organization such as a cyber command. The study excludes the use of cyber capabilities for political or economic espionage, as well as instances of cybercrime, for methodological reasons. Focusing on military operations also excludes non-state actors, which makes the research more manageable.

A. Strategic Level

Many inter-state cyber operations happen at the strategic level. Most of them are intentionally designed to stay below the threshold of an armed attack to avoid escalation into conventional conflict (Valeriano and Maness 2015, 183). To this date, there is no case of a coordinated, strategic cyber war campaign against another state that reached the level of an armed attack or could be easily classified as war. The closest to this is the planned operation Nitro Zeus, by US Cyber Command against Iran, that was uncovered in 2016. This was a contingency plan in case its predecessor, operation Olympic Games, better known as Stuxnet, and diplomatic efforts to limit Iran's nuclear program, failed. According to David Sanger, the plan included striking at Iran's air defense, transportation, and communications systems, as well as crucial parts of the power grid (Sanger and Mazzetti 2016). The pre-emptive attack would almost certainly have affected civil critical infrastructure in peacetime. Nitro Zeus was a large-scale effort involving thousands of intelligence personnel who placed backdoor implants in Iranian computer networks, preparing the battlefield. Insiders describe it as "a huge, expensive undertaking, beyond the reach of anyone but a few nation-states" (Sanger 2018, 45). Like Stuxnet, it probably required years of preparation, reconnaissance, simulation and malware testing. The plan was never executed, and one can only speculate as to why.

Fear of retaliation in the context of vulnerability of US critical infrastructures is certainly one explanation. Iran's cyber corps attacked US financial institutions after Stuxnet was uncovered (Sanger 2018, 46). Such a large-scale strategic attack would most likely be regarded as the use of force in international law and thus likely escalate into a conventional conflict in the region. Additionally, with complexity comes uncertainty about the reliability of implants that must remain undetected by adversaries for some time. Then there is the risk of collateral damage. In addition to these issues, Nitro Zeus clearly shows one benefit of strategic cyber warfare, and that is having another option on the table, in case negotiations break down (Smeets 2018b, 97). Press reports are unclear whether Nitro Zeus was conceived as a stand-alone, strategic operation that would shut down Iran's system "without firing a shot" and thus without risking the lives of US troops in a probably lengthy war (Sanger and Mazzetti 2016). It also could have been conceived as a pre-emptive first strike of a more conventional conflict. Both options are conceivable.

In academia, skeptics argue that even in war, the strategic utility of military cyber operations is limited. Martin Libicki maintains that strategic cyber attacks cannot be used effectively for two key elements of war, namely permanently disarming or degrading enemy conventional forces or occupying and holding a territory (Libicki 2009, 59). A central issue of cyber in war is that strategic cyber capabilities are target-dependent, in that they need to be tailored to specific target configurations. Because malware must be custom-built, it is more difficult to have stockpiles that are up-to-date once conflict occurs. Tomahawk missiles are built once and are ready to use during their expected shelf-life of 30 years (Defense Industry Daily 2020); but 0-day vulnerabilities have a shorter life cycle and shelf-life and they cannot be stored in the same way (Ablon and Bogart 2017). Therefore, 0-day malware must be written beforehand to be operational once fighting breaks out. Therefore, wiping-out an entire country with strategic cyber attacks requires a concerted and simultaneous effort of different attack vectors that need to be prepared and maintained in advance. This requires a huge logistical effort of keeping track of the status of implants and especially how different attack vectors are intertwined or depend on each other. High-value targets, such as critical infrastructures and command and control systems, are often air-gapped and require specialized intelligence to gain access. In many instances, this requires time-consuming social engineering in advance to gain a foothold on a system. This implies high operational complexity for a vast-scale strategic attack that permanently disrupts another country over a sustained period. Since the damage of cyber attacks is often temporary and reversible, additional resources need to be continuously spent to shut down a nation permanently (Smeets 2018a). This reduces the strategic utility of cyber capabilities in war (Borghard and Lonergan 2017, 477) and suggests that strategic cyber attacks may be valuable only in the early stages of a conflict, for example, to generate surprise effects. Cyber attacks tend to be most effective when they are not expected (Kostyuk and Zhukov 2017). In the early stages of a conflict, malware arsenals are stacked up and 0-day vulnerability arsenals are not yet burned. The longer a conflict lasts, and the longer cyber barrages endure, the fewer available 0-day vulnerabilities should remain and the lower the expected utility of cyber operations.

Another argument against the utility of strategic cyber operations comes from research on strategic air-power. Proponents of strategic bombardments of cities in war argue that pain inflicted on the adversary's population will help to turn it against its government, thereby reducing the enemy's will to resist. Empirical studies find that strategic air-raids against civil infrastructures rarely produce this effect. In contrast, attacks against civil infrastructures are often perceived as illegitimate. Instead of reducing the enemies' will to resist, they inflict anger and create a rally-around-the-flag-effect, where the population moves to support the war efforts of its government (Pape 1996). Reasoning by analogy, the same might be true for a military cyber operation that shuts down an entire nation (Lawson 2013, 94–95).

One generally assumed advantage of strategic cyber operations is that they provide military planners with a flexible instrument that can be adjusted to the specific target. Max Smeets argues that, like a covert operation, they provide state leaders with an alternative option to act without necessarily risking escalation into a physical conflict (Smeets 2018b, 97). In times when there are only bad options available, cyber solutions might be the lesser evil, because, if used cautiously, they provide states with plausible deniability and an alternative to conventional strikes or the deployment of special forces. Strategic cyber attacks can be designed to create only temporary and reversible effects; they might provide a non-lethal option as well. Reversible damage might be an option for more humane conduct of war, but risking enemy recovery might not be in the military's interest. In situations of doubt, shooting a missile and permanently destroying a military target seems to be preferable to temporary denial (Kaplan 2016, 57).

B. Operational Level

In contrast to the strategic level, there are examples of the operational use of cyber capabilities in conflict. Five cases come to mind: Syria 2007, Georgia 2008, Ukraine 2014–, Syria 2013– and one case of non-use of cyber capabilities in Libya 2011.

Operation Orchard (also known as Operation Outside the Box) took place in Syria in 2007, in which Israeli hackers disabled a Syrian anti-aircraft radar in Tell Abyad and then, in quick succession, launched a kinetic air-strike. The Israeli air force then destroyed a nuclear test site in Deir ez-Zor in northern Syria. The operations were successful and the digital component played a significant role in allowing Israeli F-15 jets to enter airspace unnoticed (Rid 2012, 19). Operation Orchard is an example of the sequential use of cyber capabilities as an "enabler" for kinetic operations, as well as a first-strike use. In such a case, the cyber operation produces an effect that is necessary for a subsequent kinetic operation.

The opposite is the joint or synchronous use of kinetic and cyber capabilities in the same context, where both components perform different functions. The Russian invasion of Georgia in 2008 and the conflict in eastern Ukraine (2014–present) are examples. The physical component of the Georgian conflict officially began on 7 August 2008 over a dispute in South Ossetia. Three weeks before this, the Georgian government and financial sector websites, along with various communication platforms, were hit by distributed denial of service (DDoS) attacks. This was a dress rehearsal for another wave of cyber attacks that were carried out simultaneously with the invasion of Russian combat troops. This time the goal was to impair Georgian communication with the outside world. Targets in the Georgian city of Gori, such as local news sites, were crippled by DDoS attacks just before Russian planes reached the city (Hollis 2011). In addition, an information operation component in the form of defacement of Georgian websites was used to spread chaos and uncertainty. Critical infrastructures, however, were not attacked. The complexity of these attacks can also be described as low. The Georgia incident demonstrates the lead time that cyber operations must have in order to be effective (Hollis 2011).

Integrating conventional and cyber operations to create joint effects is a challenge that many cyber powers are currently trying to figure out. A study by Nadiya Kostyuk and Yuri Zhukov, examining the use of cyber and kinetic military operations in Syria (2013) and Eastern Ukraine, shows that timing often does not work in sequential or synchronous operations. Between 2014 and 2016, more than 1,841 cyber attacks and more than 26,289 kinetic operations were measured in Ukraine, but only a few of them occurred simultaneously. Instead of working together, physical and cyber operations took place largely separate from another, not creating joint effects. There was no reciprocity or strategic interaction between the two forms of attack. There was also no visible correlation between successful digital attacks from one side and kinetic counter-reactions from the other. This suggests massive synchronization problems and a low military shock effect (Kostyuk and Zhukov 2017). James Lewis argues that Russian cyber operations in Ukraine have failed to produce tactical or operational military effects beyond an initial tactical surprise effect (Lewis 2015). However, psychological effects, like sowing confusion and uncertainty, might be desired effects of cyber operations. Similar findings could be replicated in the Syrian conflict in 2013 (Kostyuk and Zhukov 2017). This suggests that operational cyber capabilities are (at the moment) an ineffective tool for exercising power in conflicts. However, if forces continue to train and exercise joint operations, this might change in the future. Coordination seems particularly challenging for states that rely on external proxy actors for cyber attacks, as was potentially the case in Ukraine.

To better understand the limitations of cyber operations on the operational level, it is worth looking at a case of non-use of cyber capabilities. Shortly before the start of the NATO operation to implement a no-fly zone in Libya in 2011 (Operation Odyssey Dawn), the US discussed the use of cyber operations but ultimately decided against it. The aim was to disable the Libyan air defense, which posed a threat to NATO aircraft. According to a New York Times report, the goal was similar to Operation Orchard: to disable or jam air defenses (Schmitt and Shanker 2011). The plan was rejected for several reasons. Firstly, the Obama administration feared that it would set a precedent that would have legitimized comparable actions by Russia and China. Second, the Americans did not have enough preparation time. This confirms the previously mentioned “cold-start problem” of cyber capabilities. The US Cyber Command did not have targets to strike or suitable malware for the relatively antiquated Libyan air defenses. Thirdly, it was uncertain whether such cyber attacks could have been carried out sustainably over a longer period. There were also doubts about whether cyber capabilities could reliably disable air defenses. There is also always a degree of uncertainty around whether a disabled system may recover more quickly than anticipated. Hence, large-scale cyber operations with a kinetic component, such as Stuxnet, have to be tested in simulated environments. This has implications for cyber warfare, where there is often no time for testing. If it is difficult to assess the impact of a cyber operation, military planners are hesitant to use it. If they have the alternative of destroying an asset permanently instead of using a potentially unreliable cyber capability, they tend to choose the former (Fink, Jordan, and Wells 2014). This is why the Libyan air defense system was permanently eliminated with cruise missiles.

Lastly, there was a desire not to waste highly complex and costly US cyber capabilities on the relatively low-tech Libyan forces and run the risk of their exposure (Schmitt and Shanker 2011). Cyber operations like Stuxnet have shown that there is a risk of losing assets because of malware spreading in an uncontrolled fashion.

C. Tactical Level

Not much is known about the tactical use of cyber capabilities; however, journalist Shane Harris has done extensive research on the use of offensive tactical cyber operations during counterinsurgency operations in Iraq in 2007 (Harris 2015). This operation had three components. First, the NSA correlated the phone metadata of Iraqi internet service providers with geographic maps and thus was able to pinpoint the geolocation of mobile phones used to trigger improvised explosive devices (IEDs). The NSA was able to destroy some of these from afar or to get the location of insurgents close by (Harris 2015, 69–72). This is an instance of tactical cyber as a counter-force capability.

The second component of the operation involved the use of malware against the insurgency's computer systems. Two variants were used here. The first involved the large-scale infection of numerous Iraqi users via manipulated phishing emails. The second involved the targeted infection of computers via USB sticks, which were carried by tactical cyber units in the field. The aim was to compromise the enemy information and communication or command and control network *Obelisk*, a kind of Al Quaeda Intranet (Harris 2015, 31).

The third component consisted of information operations against insurgents. With access to the Iraqi telephone network, US troops sent fake text messages to insurgents to demoralize them or to set a trap. For example, meetings were arranged where the person who appeared was captured. Malware was also used to locate individuals who uploaded propaganda videos via internet cafés (Harris 2015, 3–25).

Tactical cyber operations are subject to numerous restrictions, which explains why they have been used only sparsely. In most cyber nations, the use of offensive capabilities is decided at the strategic level, i.e. at a high point in the military chain of command. However, strategic cyber capabilities cannot simply be converted for tactical use at lower echelons in the chain of command because the use context is different (Metcalf and Barber 2014). Tactical cyber operations are difficult to integrate into the traditional target cycle of conventional forces due to their long planning and development time. Traditional weapons only need to be targeted once; tactical cyber operations must provide permanent covert access to a hacked system. However, this can be discovered by the defender, which can lead to a loss of access. Tactical cyber operations are therefore far more resource-intensive in their planning (Fink, Jordan, and Wells 2014). The probability of discovering a hidden capability also influences their modality of deployment. It is pointless to invest large sums of money in a covert, tactical capability if it becomes uncovered in the first mission and thus becomes ineffective. Confidentiality requirements and tactical deployment have always been in conflict, as in combat situations, for example, the equipment can be captured by the adversary.

Unlike micro drones, mortars or anti-IED devices, tactical cyber capabilities are difficult to standardize, package and carry around. The tailoring requirement of cyber capabilities is a contradiction to the requirements of troops in the field. They need tools that must be repeatedly and reliably usable: an anti-IED device that only works against a certain type of mobile phone is less valuable than one that works against all types of mobile phones. Due to these characteristics of cyber capabilities, they are less suitable for tactical units (Porche et al. 2017, 47–50).

As with all cyber capabilities, collateral damage is difficult to anticipate. It is conceivable that tactical cyber operations in the field against computers of insurgents could also affect all other computers worldwide that have a similar configuration. In addition, civil infrastructure can be unintentionally affected, which can quickly become a PR disaster in tense foreign missions where the population is critical of foreign forces (Porche et al. 2017, 47–50). Tactical deployment can thus strategically escalate, for example, if collateral damage occurs worldwide. The general problem is that cyberspace does not match the geography of the battlefield on the ground. Conventional operations may be locally limited, but cyberspace is not (Metcalf and Barber 2014).

Lastly, lessons learned in Afghanistan and Iraq show that in difficult environments, such as vast landscapes and deserts, technology tends to fail. For tactical cyber operations to work, a data connection with enough bandwidth must exist. Computers need electricity and therefore they tend to be unreliable in combat situations, especially if the adversary possesses electronic warfare capabilities. Rebel forces with AK-74 rifles and almost no digital infrastructure still tend to be the most likely adversary in most asymmetric conflicts, and tactical cyber is limited against these common adversaries. For cyber operations in the field, certain proximity to the target is usually required. An enemy WLAN can only be hacked within the radio wave range. Tactical cyber operations in the field therefore only make sense if there is spatial proximity (urban warfare), if the desired effect can be standardized and thus made repeatable, if the required expertise is not too high, and if the effects can be limited to the local proximity.

4. DISCUSSION

The preliminary conclusion is that two major variables affect the utility of cyber technologies in war: the *timing* and operational *complexity* of cyber operations. Timing refers to questions of when and how long to engage in cyber operations to maximize effects. Operational complexity describes how hard it is to pull off the entire operation. Operational complexity includes various aspects such as the number of targets (one system vs. hundreds of systems to be hit at the same time), the defense level of the targets (multiple open attack surfaces vs. air-gapped systems), the availability of resources (intelligence and malware stockpile) as well as the size and internal organization and coordination of attacker teams.

Hypothesis 1: First-strike and sequential use of cyber capabilities seem easier to pull off, even for low-capacity actors, because the force-synchronization required for parallel use is hard to achieve.

In most of the analyzed cases, cyber attacks have been used in the early stages of a conflict. Cyber as a first-strike option in a conflict seems more promising and easier to pull off than continuous use in an ongoing conflict. Cyber attacks usually work best when they are not expected and when the adversary is unprepared. Continuous use requires a streamlined malware development cycle and enough personnel to rewrite malware after it gets burned or patched. If more malware gets burned than is reproduced, an operation is expected to slow down.

One aspect of operational complexity is the *availability of intelligence* that is needed to gain access to any hard-to-hit targets, especially military ones. The cases of non-use show that if there is no reliable intelligence on targets, cyber operations become riskier and less feasible. Intelligence collection and network reconnaissance involve an often time-consuming process, especially against highly secure, air-gapped targets, where in some cases, human intelligence is required. Even large cyber forces cannot prepare against any conceivable adversary, especially considering non-state actors and cyber proxies of which often little intelligence exists.

Hypothesis 2: The more preparation time there is, the more likely is the success of a cyber operation.

The case of Libya showed that if an attacker does not have time to tailor attacks for the specific targets, cyber operations are not feasible. Likewise, in rapidly unfolding crisis situations where there is no time to prepare and train, cyber tends to be of limited utility. Strategic cyber attacks aimed at shutting down an entire nation require large amounts of preparation time, as Nitro Zeus showed. But also, the cyber attacks against

Georgia had to be prepared and tested weeks in advance. How long it takes to prepare a cyber operation is also a function of the organization of one's cyber forces. Larger teams can probably produce greater malware stockpiles in a shorter amount of time and thus may need less preparation time compared to smaller teams. Larger teams, due to division of labor and functional differentiation, can also undertake multiple tasks or phases of an operation, such as reconnaissance and malware writing and testing, more efficiently, whereas smaller attack teams probably face some restrictions in the number of targets they can penetrate simultaneously or over a sustained period. Of course, this depends on their effectiveness and the structure of their organization. However, larger attack teams are potentially harder to synchronize than smaller teams. If states rely on external proxy actors like patriotic hackers, it may be harder to synchronize and control their attacks. The more actors are involved in a cyber operation, the higher the complexity becomes.

Hypothesis 3: High operational complexity increases the risk of failure of any sustained cyber campaign.

Coordination of two military components, such as a cyber force and an air force, in one single operation against one target, like Operation Orchard, seems manageable. The more military components or organizations that come into the loop, the harder it becomes to coordinate them. The more actors are involved and the longer an operation lasts, the more complex it tends to get. The broader the scope of the operation, i.e. striking a single target vs. striking an entire nation over a period of time, the more complex the operation. The same is true for targets with broader attack surfaces. As many IT-systems are interdependent, there is always a risk of unexpected collateral damage when shutting these down with cyber attacks. As in any complex system where the interaction of the different individual parts is non-linear and opaque, it is hard for external observers to make predictions. Thus, the more complex cyber operations get, the harder it becomes to predict outcomes, and thus the higher the uncertainty and the lower the ability to guarantee success.

Hypothesis 4: If military commanders have alternative options to cyber operations with high complexity and thus uncertain reliability, they tend to choose the safer option (that is, using kinetic means to disable targets instead).

The high degree of uncertainty of complex cyber operations also influences the use decision of commanders. Libya and Nitro Zeus showed these signs of hesitation. Since the damage of cyber attacks is often temporary, there is always a risk of unanticipated resilience. A shut-down system can come back online quicker than anticipated. However, if a cyber attack is the first step in a whole military war plan and this step fails, the rest of the planning that depends on the effects of the first cyber attack is at risk. Therefore, traditional means of physically destroying targets may seem more reliable.

These hypotheses will be tested in future research. The preliminary conclusion is that the argument of the all-purpose sword does not hold up completely. Cyber technologies in war certainly have some benefits, but a lot of operational hurdles need to be overcome for them to become a perfect all-purpose sword. Right now, it seems that cyber operations are more like a specialized weapon for quick strikes, rather than for lengthy and sustained campaigns. They require a lot of training and preparation and are difficult to wield together with another type of arms. As with all weapon types, in the end, the organizational structure and the tactics used are what determines the success rate of any given weapon.

REFERENCES

Ablon, Lillian, and Andy Bogart. 2017. *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits*. Research report RR-1751-RC. Santa Monica, Calif: RAND. https://www.rand.org/pubs/research_reports/RR1751.html.

Arquilla, Jon. 2017. “The Rise of Strategic Cyberwar?” https://cacm.acm.org/blogs/blog-cacm/221308-the-rise-of-strategic-cyberwar/fulltext.

Bateman, Robert. 2015. “Understanding Military Strategy and the Four Levels of War: When ‘Strategy’ Gets Thrown Around by Politicians and the Media, You Can Bet It’s Being Misused.” https://www.esquire.com/news-politics/politics/news/a39985/four-levels-of-war/.

Borghard, Erica D., and Shawn W. Lonergan. 2017. “The Logic of Coercion in Cyberspace.” *Security Studies* 26, no. 13: 452–81. https://doi.org/10.1080/09636412.2017.1306396.

Clausewitz, Carl von. 1982. *On War*. Reissued. Penguin Classics. London: Penguin Books.

Crane, Alfred C., and Richard Peeke. 2016. “Using the Internet of Things to Gain and Maintain Situational Awareness in Dense Urban Environments and Mega Cities.” *Small Wars Journal* (February).

Defense Industry Daily. 2020. “Tomahawk’s Chops: XGM-109 Block IV Cruise Missiles.” https://www.defenseindustrydaily.com/block-iv-xgm-109-tomahawk-chopped-07423/.

Fink, Kallie D., John Jordan, and James E. Wells. 2014. “Considerations for Offensive Cyberspace Operations.” *Military Review* (May-June).

Gartzke, Erik. 2013. “The Myth of Cyberwar: Bringing War in Cyberspace Back down to Earth.” *International Security* 38, no. 2: 41–73. https://doi.org/10.1162/ISEC_a_00136.

Harris, Shane. 2015. *@War: The Rise of the Military-Internet Complex*. First Mariner Books edition. Boston, New York: Mariner Books Houghton Mifflin Harcourt.

Hollis, David. 2011. “Cyberwar Case Study: Georgia 2008.” *Small Wars Journal*. https://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008.

Jun, Jenny, Scott LaFoy, and Ethan Sohn. 2015. *North Korea’s Cyber Operations: Strategy and Responses*. Washington, DC, Lanham, Boulder, New York, London: Center for Strategic & International Studies; Rowman & Littlefield.

Kaplan, Fred M. 2016. *Dark Territory*. New York: Simon & Schuster Paperbacks.

Kostyuk, Nadiya, and Yuri M. Zhukov. 2017. "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?" *Journal of Conflict Resolution* 63, no. 2: 317–47. https://doi.org/10.1177/0022002717737138.

Lawson, Sean. 2013. "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats." *Journal of Information Technology & Politics* 10, no. 1: 86–103. https://doi.org/10.1080/19331681.2012.759059.

Levy, Jack S. 2008. "Case Studies: Types, Designs, and Logics of Inference." *Conflict Management and Peace Science* 25, no. 1: 1–18. https://doi.org/10.1080/07388940701860318.

Lewis, James Andrew. 2015. "'Compelling Opponents to Our Will': The Role of Cyber Warfare in Ukraine." In *Cyber War in Perspective: Russian Aggression Against Ukraine*, edited by Kenneth Geers, 39–48. Tallinn, NATO CCDCOE.

Libicki, Martin C. 2009. *Cyberdeterrence and Cyberwar*. Santa Monica: RAND Corporation. http://swb.eblib.com/patron/FullRecord.aspx?p=566752.

Metcalf, Andrew, and Christopher Barber. 2014. "Tactical Cyber: How to Move Forward?" https://smallwarsjournal.com/jrnl/art/tactical-cyber-how-to-move-forward.

Pape, Robert Anthony. 1996. *Bombing to Win: Air Power and Coercion in War*. 1. publ. Cornell Studies in Political Economy. Ithaca, NY: Cornell University Press.

Porche, Isaac, Christopher Paul, Chad C. Serena, Colin P. Clarke, Erin-Elizabeth Johnson, and Drew Herrick. 2017. *Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below*. Research report RR-1600-A. Santa Monica Calif. RAND.

Rid, Thomas. 2012. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35, no. 1: 5–32. https://doi.org/10.1080/01402390.2011.608939.

Sanger, David. 2018. *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. New York, Melbourne, London: Crown Publishers; Scribe.

Sanger, David, and Mark Mazzetti. 2016. "U.S. Had Cyberattack Plan If Iran Nuclear Dispute Led to Conflict." *New York Times*, February 16. https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html.

Schmitt, Eric, and Thom Shanker. 2011. "U.S. Debated Cyberwarfare in Attack Plan on Libya." *New York Times*, October 17. https://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html.

Smeets, Max. 2018a. "A Matter of Time: On the Transitory Nature of Cyberweapons." *Journal of Strategic Studies* 41, no. 1-2: 6–32. https://doi.org/10.1080/01402390.2017.1288107.

Smeets, Max. 2018b. "The Strategic Promise of Offensive Cyber Operations." *Strategic Studies Quarterly* (Fall): 90–113.

US Air Force. 2019. "Annex 3-70-Stragegic Attack." https://www.doctrine.af.mil/Doctrine-Annexes/Annex-3-70-Strategic-Attack/.

Valeriano, Brandon, Benjamin M. Jensen, and Ryan C. Maness. 2018. *Cyber Strategy: The Evolving Character of Power and Coercion*. New York, NY: Oxford University Press.

Valeriano, Brandon, and Ryan C. Maness. 2015. *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*. New York, NY: Oxford University Press.

van Haaster, Jelle. 2019. *On Cyber: The Utility of Military Cyber Operations During Armed Conflict*, Amsterdam, University of Amsterdam.

Young Kong, Ji, Kyoung Gon Kim, and Jong in Lim. 2019. “The All-Purpose Sword: North Korea’s Cyber Operations and Strategies.” In *11th International Conference on Cyber Conflict: Silent Battle*, edited by T. Minárik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga, and G. Visky, 143–62. Tallinn: NATO CCD COE Publications.