2018 10th International Conference on Cyber Conflict
CyCon X: Maximising Effects
T. Minárik, R. Jakschis, L. Lindström (Eds.)
2018 © NATO CCD COE Publications, Tallinn

Targeting Technology: Mapping Military Offensive Network Operations

Daniel Moore
Department of War Studies
King's College London
London, United Kingdom
daniel.d.moore@kcl.ac.uk

Abstract: State-sponsored network intrusions are publicly and frequently exposed but assessing how militaries conduct offensive network operations remains difficult. Data can be transmitted near-instantaneously, yet cyber-attacks can take months or even years to mature, complicating attempts to integrate them into joint operations. What challenges, risks, opportunities and advantages are associated with attacking networks? This paper argues that military offensive network operations can be usefully cast into a two-part taxonomy: event-based attacks and presence-based attacks. These are then applied to practical use-cases drawn from existing strategies, case studies and current military platforms. Event-based operations include all instances in which the target is directly and in real time attacked by compromise of its software and may appear roughly analogous to physical weapons. Presence-based operations include all network intrusions in which the attackers traverse compromised networks until targets are located, assessed, and weaponized for later activation, more analogous to a clandestine sabotage operation. Distinguishing between these two types is crucial; they offer different solutions, encompass varying risks, and may require different resources to accomplish. Event-based attacks can offer a tactical advantage against a single adversary platform or network. A successful presence-based operation may result in a strategic advantage against a stronger force. Each of the two operation types is broken into phases as defined by the US Department of Defense Common Cyber Threat Framework. The model envisions four steps in the network operation life-cycle: preparation, engagement, presence and effect. By anchoring the assessment using the framework, the unique characteristics of both operation types become easier to analyze.

Keywords: *cyber warfare, network operations, cyber attacks, offensive cyber*

1. INTRODUCTION

Military use of offensive network operations (MONOs) epitomizes the desire for cleaner, quicker, and less violent conflict. If strategic adversary coercion can be achieved by targeting the digital infrastructure used for both national security needs and daily life, enemy resolve should theoretically decrease to the point of surrender. This is an understandably appealing concept, but not entirely accurate. Network operations can assist both tactical and strategic combat efforts if all their particular advantages and disadvantages are accounted for. While nations occasionally release slivers of information on how they employ offensive network capabilities, doctrine and strategy remain understandably murky on how operational success is achieved in and through networks.

At the core of this work is the argument that *MONOs can broadly be grouped into two classes;* ***presence-based*** *and* ***event-based***. Presence-based operations are offensive network activities which include a lengthy intrusion component meant to establish a persistent presence within adversary assets, and then traverse networks and locate objectives. Event-based operations primarily include direct attacks intended to cause immediate effect against a targeted platform. Many of the currently known state-sponsored network attacks would fall into the former category, while many network attacks against military hardware and software in the battlefield would fit the latter. All can be carried out for military objectives.

A typology for network warfare matters. When all offensive operations are assessed together, the results often seem muddled and difficult to translate to military doctrine.[1] Examined separately, presence- and event-based operations are shown to have distinctive characteristics embodying unique advantages and disadvantages. They require different manpower, resources and operational approaches, and can be applied against different targets for different effects. Some may be more easily relegated to battlefield use, while others are best kept for strategic maneuvers. Activating a presence-based operation may entail losing a crucial source of intelligence, while event-based attacks are inherently suitable for recurring military use. By identifying the parameters under which an operation or capability can be relegated to each of the categories, it empowers decision-makers to "release" some capabilities to battlefield commanders, while retaining sensitive measures within the higher echelons.

Event-based operations are roughly analogous to firing a weapon. When such an attack is launched, virtual ordnance traverses one or more networks, where it connects with the adversary's defenses. Impact on the target – if successful – is immediate or near-immediate. They are meant to be reusable, and the attack may be launched by a local fire team, a warfighting platform or from remote territory. These types of attacks – like

1 For an example of the deliberations around these challenges, see Atkin, McLaughlin, and Moore (2016).

their kinetic counterparts – often have localized effects meant to augment or support kinetic strikes (US Army 2014, 31). They may disrupt an aircraft's onboard systems, degrade radar functionality or impair a regional network by way of a destructive worm that wipes endpoints and servers. As a corollary, such tactical network warfare works well in a combined arms package, jointly deployed alongside kinetic capabilities.

Presence-based operations are roughly analogous to clandestine sabotage operations. A precursor successful intelligence operation results in sustained remote access to an adversary's networks. From that point, attacker assets are maneuvered to enumerate servers and endpoints, gathering information and identifying weak points that may subsequently be attacked for effect. Specialized implants are fielded where needed, with the intent to activate when the order to do so arrives. This can manifest as a multi-year intrusion campaign into an adversary's command and control network, logistics framework or critical infrastructure. The potential risks to friendly weapons and capabilities of discovery are far greater due to the extended presence "behind enemy lines", as is the chance of failure. But the potential benefit is commensurately immense, possibly resulting in an advantage of strategic proportions. These operations may serve as the surprise prelude to an offensive campaign or as a means of exerting pressure on adversary governments.

This article offers an in-depth analysis of MONOs for both event-based and presence-based attacks. The model chosen as the theoretical scaffolding is the US Department of Defense's *Common Cyber Threat Framework* (US DNI 2013), which capably aggregates different industry and public-sector models to provide a useful approach towards assessing wider network campaigns rather than focusing on individual intrusions. The four primary phases presented in the Common Cyber Threat Framework – *preparation, engagement, presence, and effect* – are assessed for both presence and event-based operations.

While official information on MONOs is scarce, this does not imply a dearth of sources. The increasing tenacity of the information security industry in unravelling nation-state cyber capabilities provides a useful window into well-resourced network operations. Industry network defenders working to deconstruct organized adversaries have generated useful analytical models such as Lockheed Martin's Cyber Kill Chain (Hutchins, Cloppert, and Amin 2011) and the Diamond Model (Caltagirone, Pendergast, and Betz 2013). Official publications do indeed exist, and include tactical accounts of how units operate on the field (Kimmons 2017), joint publications on doctrine (US Joint Chief of Staff 2013), strategic guidelines (Chairman of the Joint Chiefs of Staff 2006), oversight reports (US DoD 2017) and even operational integration roadmaps (US DoD 2003). Although employed cautiously, even leaks

of highly-classified materials from network operations units such as the NSA[2] can contribute information on context and capabilities.

Military network operations do not exist in a vacuum. In contrast to some existing models, they do not begin with target reconnaissance and do not end after activating offensive payloads (Hutchins, Cloppert, and Amin 2011, 4–5). There are several strategic and tactical phases predicating the operation itself, and several that follow it. Similarly, there are processes that run concurrently to the network intrusion, interacting with work carried out by network operators to facilitate their success and feeding off it. These additional components are not peripheral; they are instrumental to an operation's success and are an integral part of understanding offensive military capabilities in cyberspace.

Some limitations accompany the scope of this work. Firstly, while the sources and case studies below are not limited to the US, they do favor them significantly due to their relative availability. Secondly, the proposed distinction is meant as a useful generalization for the allocation of resources and division of forces rather than a catch-all classification. Some niche cases may not fall neatly within one category or the other, and some attacks may present elements of both, such as a presence-based intrusion which is then used to launch subsequent event-based attacks.

2. PREPARATION

Preparation encompasses all efforts preceding contact with the enemy. The Cyber Threat Framework defines preparation as all collective efforts to identify targets, develop capabilities, assess victim vulnerability and define the scope of the operation (US DNI 2013, 2). Each of these processes reflects months and perhaps years of investment in resources, both material and operational. Thus, while it is the least discussed, the preparation phase of any offensive network operation may often be its longest.

Before operators first interact with adversary networks, planners must first initiate a *targeting* cycle. This may seem deceptively trivial; an actor seeking to target an adversary will simply pursue its networks. In reality, locating, identifying and enumerating relevant networks for attack can be difficult (Monte 2015, 20). Modern militaries employ dozens of disparate networks even within a single organizational entity (Burbank et al. 2006, 39–42). Identifying which to attack is no negligible feat. It requires in-depth intelligence and an understanding of the adversary's order of battle. In many cases, sensitive or operational networks do not interface directly

2 There were at least three separate leaks in the US alone. These include NSA leaks by former contractor Edward Snowden and by a group calling itself the Shadow Brokers in 2016, and a purported CIA leak in 2017, see Wikileaks (2017, 7).

with the Internet or perhaps even with any other networks.[3] This makes the notion of identifying them and securing access that much harder. The force commander will choose to pursue a target through networks only if it is deemed to be the most effective means of attaining the objective (Ducheine and van Haaster 2014, 313–14).

Targeting cycles are decidedly different for presence and event-based operations. Targeting for presence-based operations is most commonly conducted by the strategic intelligence entities that have network intrusion capabilities. Traditionally, it is within the remit of signals intelligence (SIGINT) organizations, which in varying jurisdictions are either civilian or military.[4] As such, it is often a derivative component of those entities' prioritized intelligence requirements (PIRs). PIRs form a fundamental national security agenda towards which agencies are expected to work, whether by collecting intelligence or preparing for eventual network attacks (US DoD 2013, 24–25). Targeting is therefore a long-term process in which intelligence on the adversary is accumulated, increasingly providing information required to properly prioritize between networks by balancing feasibility and relevance to the objectives at hand. The result is a highly curated list of specific targets.

Targeting for event-based operations would reasonably take place in proximity to the attack itself (Conti and Raymond 2017, 181–82). As a result, this cycle could commonly be conducted by the theatre force commander, or perhaps even a tactical unit lead against a limited objective. This, alongside the employment of pre-packaged network capabilities, entails that the decision-making process is both faster and conducted with far available resources. In order to identify which networks should be selected for subsequent engagement, the commander must identify the adversary's local centers of gravity which, if compromised, would reduce enemy effectiveness. To accomplish this, reconnaissance assets conducting spectrum analysis and automated network mapping procedures may identify adversary networks in the region, possibly even auto-assigning ordnance against them.

Some targets may be chosen for both event and presence-based operations, reflecting varying goals and opportunities. Over the last two decades, the United States has gradually modernized battlefield connectivity for its deployed forces. A part of this process, titled Warfighter Information Network – Tactical, or WIN-T, is a prime example of how saturated the network landscape can be. A combination of dedicated line-of-sight radios and satellite-communication terminals (Coile 2009, 5) services a host of networks including the general-purpose NIPRNet, SIPRNet[5], and local compartmentalized data and voice networks (Epperson 2014). Many of these

3 The idea of separating a network from all other networks is called "air-gapping" and is a widely accepted methodology of reducing a network's potential attack surface.

4 In the United States, the NSA is a civilian agency. In the Israeli example, it is military unit 8200.

5 Non-Secure Internet Protocol Router Network (NIPRNet) and Secure Internet Protocol Router Network (SIPRNet): US Department of Defense networks used for unclassified and classified communications between and within partner organizations.

networks enable unclassified, ancillary functions that are not mission critical. Others carry sensitive targeting information, communications or intelligence data. Some of these networks may be inaccessible as they are transmitted over a medium to which the attacker has little hope of gaining access. Others rely on commercial satellites and even the Internet as their transmission medium. Completing the targeting process by successfully classifying which networks both matter and are pragmatically reachable is therefore a challenge. In some cases, these networks may be subjected to long-term compromise in the form of a presence-based operation. In other cases, locally accessible datalinks such as a regional network cell might be the target of an event-based attack. Interestingly, the WIN-T project has now been officially terminated by the US military, citing concerns that the project's architecture is indeed too vulnerable to a determined, well-resourced adversary (Crawford, Mingus, and Martin 2017, 6–8).

One crucial pre-operation process is *capability acquisition and development*. Capabilities in network warfare include all hardware and software used to affect enemy platforms. There is some limited merit in downplaying the complexities of this process; unlike actual weapons, network intrusion tools can ostensibly be developed by anyone. Similarly, the development cycle for a potent so-called "cyber-weapon" is also typically deemed to be much shorter (Rattray 2001, 171), easier and cheaper (Nye 2010, 5). Again, there is some reason to this assertion. However, the unique circumstances of developing capabilities to attack networks are well worth examining. Each supposed advantage is mirrored by an equal or greater disadvantage.

Presence-based attack tools must be stealthy, agile, and modular. They must be stealthy as the majority of their life-cycle will be spent clandestinely embedded in adversary networks. They must be agile to enable operators to use them creatively to traverse adversary networks, collect intelligence and weaponize valuable targets. Finally, they must often be modular to allow operators to only deploy necessary capabilities at any given moment, thereby reducing the footprint of the tool, a further operational security mechanism (Monte 2015, 124). Each deployment of a highly engineered network attack tool must be carefully managed to include only the components currently needed to facilitate success. The expectation that presence-based operational tools must be stealthy introduces a significant weakness: these tools become quite brittle in use. The pervasive notion that offensive network tools are single-use stems from this very issue (Libicki 2009, 83). The defensive cycle for a network adversary is demonstrably shorter, as detected malware can result in detection signature within days of its discovery by a capable defender. It is not just the particular deployment that is threatened; detection of an offensive platform risks its compromise against all targets against which it is currently employed. That is a momentous risk of capabilities, which explains in part why intelligence agencies often guard them so carefully.

It is almost inconceivable that network attack tools could enjoy the same operational longevity as their kinetic counterparts. One of the longest known offensive network operations platforms – codenamed Regin by its private-sector discoverers – was ostensibly operating from at least 2003 (Kaspersky Lab 2014, 3) and widely attributed to the NSA (Rosenbach, Schmundt, and Stöcker 2015). At the time of its discovery in 2014, security company Kaspersky claimed that it was "…one of the most sophisticated attack platforms we have ever analyzed" (Kaspersky Lab 2014, 23). Once publicized and with its various mechanisms for communication and stealth thoroughly mapped and defended against, NSA operators would have had to immediately cease all intrusion activity until sufficient changes could be made and new evasion mechanisms deployed. Such an event is both an enormous investment in time and resources and also potentially a major operational compromise.

Conversely, event-based attack tools must be robust, aggressive, fool-proof and intuitive to operate. As they would likely be deployed by frontline units, no expertise must be needed to wield them effectively. They must be able to operate against a wide range of targets in a slew of contingencies, while generating similarly predictable effects. Battlefield operators will not have time to dynamically redeploy modules or carefully orchestrate network traversal. The weapon must therefore be capable of autonomously completing its objectives without further assistance. Resource exhaustion attacks, such as the often-seen denial of service attack or generic destructive payloads, are common examples of event-based capabilities.

Both presence and event-based capabilities require investment in *vulnerability research*. This entails all efforts to locate exploitable flaws in software and hardware used by the adversary: flaws that can be subverted to compromise the target and get it to either behave unexpectedly or preferably to run arbitrary code. Vulnerability research runs the gamut from generic-use software such as Microsoft Windows to dedicated software used by military hardware and other niche platforms. It is a crucial component in most network attack tools.

Software vulnerabilities are difficult to find both for attackers and defenders. From the offensive perspective, effectively exploiting critical software in a manner conducive to intrusions is increasingly difficult (Symantec 2017, 16). At the same time, there is no shortage of vulnerabilities, as data indicates that publicly disclosed, high severity submissions have nearly doubled in 2017 (NIST 2017). From the defender's perspective – as a RAND report indicated in 2017 – unless the tool weaponizing them is somehow discovered, vulnerabilities last an average of almost seven years without being exposed (Ablon 2017, 11). Thus, maintaining an expert workforce entrusted with continuously hunting for new useful vulnerabilities is paramount.

For event-based operations, the final component of preparation is integrating capabilities for use with forward-deployed warfighting platforms. Presence-based operations are often handled by remote operators, much like drones. However, in many cases, especially those involving segregated networks used to communicate sensitive data, proximity or line-of-sight access is required. In these cases, military forces may find themselves delivering fire directly in the field, be it by aircraft, naval vessel, ground vehicle or actual boots on the ground.

There are recent examples of event-based attacks in which network capabilities were supposedly integrated into battlefield platforms. The United States military operates infantry cyber teams to work alongside electronic warfare assets to map out enemy networks and identify targets (Kimmons 2017). The Russian military has, allegedly, disrupted Royal Air Force sorties over Syria by way of a network attack launched from a deployed electronic warfare vehicle (Giannangeli 2017). Developing a reliable, robust, battlefield-deployable offensive cyber capability is increasingly becoming viable, albeit expensive. Thus, while attacking networks may seem to be low-cost, attaining battlefield readiness and conducting event-based offensive operations may include hefty development, targeting and intelligence cycles.

3. ENGAGEMENT

The Cyber Threat Framework defines the initial engagement phase as: "Threat actor activities taken prior to gaining access but with the intent to gain unauthorized access to the intended victim's physical or virtual computer or information system(s), network(s), and/or data stores" (DNI US 2013, 4). Put simply, this phase embodies the attempts to intrude upon the enemy; it is the first active contact with its networks, intent on establishing a digital beach-head. What the framework obfuscates is the characteristics of this phase. Adopted from the operational typology used by Buchanan, the engagement phase may occur months in advance for presence-based operations or adjacent to the desired effect for event-based attacks (Buchanan 2017, 76–84). Not all cases are created equal, but all share one notable commonality; the engagement phase starts the operational clock.

A ubiquitous approach to network intrusion is compromising an internet-facing server or device. Identifying and compromising these may be easier than directly penetrating segregated networks, but not all such targets are inherently useful. Operations may also commence by interacting with an individual rather than a machine. Strategic network operations intended to gain entry to sensitive networks may first need to compromise those who routinely use them and hold trusted access to their assets. The reason for this is two-fold: first, there may not be a viable technological intrusion

vector, as many sensitive networks are cut off from external inputs; and second, the users are often the most vulnerable element in an otherwise secure network (Barrett 2003). They are prime targets for social engineering as an intrusion vector, but that does not mean it is always a trivial endeavor. Successfully getting individuals to usefully compromise their own security without arousing suspicion often requires expertise, preferably provided by dedicated personnel.

In event-based operations, the engagement phase can occur in seconds. As the targeting cycle is similarly shortened, there is no time to craft phishing emails tailored to human targets or set up elaborate honeypots. Instead, the engagement phase will focus on compromising accessible targets by exploiting remote software and hardware vulnerabilities. Particularly when using automated capabilities to target warfighters or other connected devices, it is sometimes possible to directly attack the software to gain entry. The engagement phase for event-based operations may not always result in full access to the target, but depending on what the desired effect is, that may not be necessary. For example, simply attempting to exhaust available resources or corrupt a target's means of communication may be possible without ever being able to execute code directly on the target and if the goal is to prevent the target from functioning as intended, that may be sufficient. Such scenarios are more easily placed within a military context; see for example denial of service attacks, which bear some similarities to conventional electromagnetic jamming.[6]

The potential perpetrators for event-based operations are far more varied than their presence-based counterparts. In many cases, these could be forward-deployed offensive cyber units, such as both the US and the UK are increasingly using (US Army 2014, 30–32). In other instances, field staff such as human intelligence assets or specific warfighters may be required to facilitate the actual engagement. As Edward Snowden revealed in a leaked top-secret document in 2013, the NSA's GENIE program to facilitate semi-automated network operations would at times rely on such assets. When necessary, field operators would physically infect adversary devices, plant hardware, or conduct short-range offensive SIGINT (NSA 2013). SIGINT agencies with global or regional reach could also deliver payloads from remote facilities.

4. PRESENCE

The presence phase is where most of the friction occurs between intruder and target. It is where persistent malicious software is continuously employed to understand, dissect, and establish a hold within the targeted network or networks, gradually extending the intruder's access until it locates servers or devices suitable to achieve the task at hand (US DNI 2013, 5). It is the process of extending and cementing

6 This aligns nicely with US military doctrine that situates Cyber and Electromagnetic Activities (CEMA) as a unified operational function, see US Army (2014).

the reach into the adversary's networks, two processes respectively called lateral movement and persistence.

The presence phase embodies the biggest discrepancy between the two operational categories – time spent on target. Where presence-based operations unsurprisingly spend most of their lifecycle in the presence phase, event-based operations may have an inconsequential or even non-existent presence phase. When nation-state intrusion campaigns are analyzed and reported to take months prior to detection, this primarily refers to the presence phase. The key difference in timespan reflects applicability to two wholly different operational tempos. For presence-based operations, the presence phase is essentially a cyclical process of expanding micro-intrusions in which additional nodes in the network are scanned, breached and subsequently assessed for mission relevance. This is represented well in the Kill Chain model, which threads multiple compromises on targeted networks into a single campaign with shared features (Hutchins, Cloppert, and Amin 2011, 7–8). Each intrusion must be handled with care to avoid tripping any alarms or informing network defenders of an active intrusion against them.

Presence-based offensive operations are first intelligence operations. Until such a time as a more active measure is needed, malicious software is tasked with either remaining dormant or collecting information, identical to the behavior in an intelligence mission (Lin 2010, 64). As a corollary, operators in the presence phase must rely extensively on the assistance of intelligence analysts to assist in further targeting and dissection of materials exfiltrated from the target (Malone 2010, 16). In some cases, the offensive is carried out entirely by the intelligence agency (GCHQ 2012). The presence phase is thus both assessing the independent intelligence value of the target, and simultaneously gathering information needed to help steer the operators towards the server or servers where attacking would result in achieving the desired objective.

When Russian operators initially infiltrated the Ukrainian power grid in 2015, they did not immediately wreak havoc on all they encountered. Instead, earlier intrusion efforts cleverly used the specialized protocols unique to these industrial networks to traverse the network, map its layout and glean the information required to develop robust offensive capabilities (Dragos 2017, 9). In a subsequent operation, the presence phase included pivoting from the power company's corporate network onto its industrial network, leveraging an attack against both to simultaneously cripple the grid and prevent operators from fixing it (Dragos 2017, 10). Finally, advancements eventually allowed the operators to "…de-energize a transmission substation on December 17, 2016" (Dragos 2017, 4) by way of the CRASHOVERRIDE malware tailored to affect even relatively well-defended energy grids. The Russians had achieved a malware-induced blackout, but they had done so after a considerable amount of time from the

initial engagement phase. Success would not have been possible without expertise and accrued experience.

For event-based offensive operations, the presence phase is nearly imperceptible. This is intrinsic to the attack vector; capabilities employed in an event-based attack are meant to impact the target directly and then disappear, leaving as few lingering artefacts as possible. Were tell-tale indicators to remain, such as residual code left running or files persisting in the target's file system, it would simplify subsequent efforts by the adversary to develop future countermeasures. Thus, it is significant for an event-based capability to be only minimally present on enemy assets.

A cascading effect – intentional or otherwise – may result in an event-based attack having a limited period of network presence. For example, an automated network attack tool designed to propagate through networks and rapidly destroy all infected endpoints and servers would require a limited presence to ensure subsequent infections of additional targets. A good example of such an attack is the NotPetya destructive malware, which in 2017 heavily affected Ukrainian networks before cascading beyond its scope to adversely affect various other entities globally (Perlroth, Scott, and Frenkel 2017). The attack, which resulted in extensive damage to victims worldwide, was unusually publicly attributed by numerous Western intelligence agencies to the Russian military.[7]

The potential cost incurred in discovery is arguably the most meaningful deterrent to attacking via cyberspace. In recent years, a growing trend amongst large vendors in the information security market has been to uncover massive nation-state surveillance efforts, often facilitated by highly sophisticated malicious software. The immediate result of this compromise is an attempted rollback of all deployed assets, both by the original offender attempting to effect damage control and the victims who enjoy updated configurations for their defensive products. The product of this is a partial collapse of the aggressor's intrusion infrastructure and, more importantly, the defender's near-immediate inoculation against future attempts to use the same tool in an offensive capacity. The presence phase is thus the most sensitive component in many offensive network operations. The continuous friction with different adversary networks and the need to collect intelligence means that discovery and eventual inoculation are a big risk to attackers. Presence operators must therefore continuously work to conceal their moves, clean up evidence and establish stable, covert communication channels that would reliably allow decision-makers to activate positioned offensive payloads when necessary (Peterson 2013, 123).

7 See, for example, US Press Secretary (2018).

5. EFFECT

The final effect phase is where triggers are pulled. Ordnance is activated, disabling, disrupting or manipulating targets. Effects either translate into objectives, fizzle uselessly, or have unintended and potentially disastrous collateral effects. For presence-based operations, the effect phase is the culmination of possibly months of planning, targeting, intelligence collection, infection attempts and dedicated development (Rattray and Healey 2010, 79). For event-based operations, the effect phase represents the primary thrust of the attack. When Richard Clarke declared in 2009 that "strikes in cyber war move at a rate approaching the speed of light" (Clarke 2009, 32), he was not referring to the entire span of an operation, but rather to the period of time between the activation of the ordnance and its detonation on the target, the manifestation of the effect phase. Even so, ordnance may be instantly triggered but may still take time to deliver its intended effect.

Distilling various official definitions, there are three "attack" types when targeting networks – disruptive, manipulative, and destructive.[8] Disruptive, or suppressing, attacks inflict "temporary or transient degradation by an opposing force of the performance of a weapon system below the level needed to fulfil its mission objectives" (US DoD 2017, 229). Their utility increased with the rise of electronic warfare, where electromagnetic transmissions could be jammed to produce a temporary but potent effect (Army Headquarters 2003, 7). The concept of disruptive attacks has made a natural transition to cyberspace, where temporarily degrading the capacity of military resources can adversely affect the efficacy of an adversary force (US Army 2014, 9).

Disruptive network attacks are commonplace even outside military scenarios. So-called denial-of-service attacks capable of levying massive throughput of network traffic routinely disrupt the functionality of online services, big and small. The targets range from global gaming communities such as the Sony PlayStation Network (Samit 2016) to major banks (Hamill 2014). Typically, these attacks either exploit an implementation flaw in the targeted technology or simply attempt to overwhelm its available resources. No legitimate connections can interact with the platform as intended, rendering it temporarily disabled for its original purpose. Similar approaches may be applied to military technology, platforms and protocols.

Manipulation effects attempt to alter information or functionality in the adversary networks, thereby deceiving operators or preventing intended system functionality. Such attacks attempt to alter perception, preventing an adversary from acting properly to further its own objectives. A scenario could include introducing a nearly imperceptible deviation to a weapon's targeting process, causing strikes to miss due

8 Adapted from the US Military's taxonomy of "…deceive, degrade, deny, destroy, or manipulate…", see US Army (2014, 17). Libicki similarly speaks of attacks aimed at eruption (target illumination), disruption, and corruption. See Libicki (2009, 145).

to what could appear to be a technical glitch. Kinetically, this is hard to accomplish but could be roughly analogized to physically tampering with a missile's warhead to secretly render it inert. When the missile fires, it seemingly behaves as normal until impact, when the warhead does not detonate. During the heat of conflict and until it happens repeatedly and consistently, it would be difficult to identify the fault as an attack. By the time it is discovered, it would likely already be too late. As the Stuxnet campaign demonstrated (Falliere, Murchu, and Chien 2011; Farwell and Rohozinski 2011), masking a manipulative effect to increase its longevity can cause an effect to be repeatedly successful over time. Hiding an effect does, however, require incrementally introducing it; an immediate and blunt change of circumstance markedly increases the probability of detection.

Destructive attacks are intended to inflict damage on adversary networks, either on hardware, software or both. These types of attacks are firmly rooted in conventional warfare, where destruction of enemy assets and personnel is often seen as the primary method of reducing its combat effectiveness.[9] When applied to network operations, a destructive attack could cause permanent software damage, such as in the case of malware which completely erases all critical files on target servers,[10] or even permanent hardware damage, such as the previously mentioned Stuxnet worm targeting the Iranian nuclear project (Langner 2011).

6. CHALLENGES AND OPPORTUNITIES

Delineating between event-based and presence-based operations allows a discussion on how militaries are integrating these capabilities into doctrine and strategy. They are markedly different in characteristics, duration, challenges, and opportunities and thus must not be lumped together, but fundamental similarities exist between the two categories and are certainly helpful in understanding networks as a medium for warfare; but useful observation of military capabilities will remain limited unless we recognize that not all capabilities must be treated the same.

Event-based operations represent the instances in which network attacks are somewhat analogous to the kinetic. Like firing a weapon, an event-based operation entails sending a payload from attacker to target in the hope of immediately reducing its integrity or capacity to operate. As a result, these capabilities are often more tactical in nature, easier to integrate with existing military OODA loops,[11] and are promising candidates for joint warfare. They are, however, limited in scope, may require extensive research

9 The classic approach to warfare - most commonly codified by Prussian strategist Carl von Clausewitz – favours destruction as the sole means of achieving military coercion. See Clausewitz (1873) for the original school of thought.

10 See, for example, the 2012 Shamoon attack, in which a presumably Iranian attacker wiped thousands of computers at Saudi's national gas company, Aramco (Bronk and Tikk-Ringas 2013).

11 OODA loop – A process in which combatants Observe, Orient, Decide, and Act. Military vernacular for conceptualising decision-making process in combat. See Boyd (1995).

and development, and could be limited to a specific subset of adversary equipment. A weapon suitable for disabling a US Navy destroyer may exploit hardware-specific vulnerabilities,[12] rendering it unsuitable against other targets. Consequently, battlefield operators deploying such weapons must have immaculate understanding of their adversary and a firm control of their own options.

Presence-based operations are intelligence missions with an offensive finisher; a form of digital sabotage. They may initially appear indistinguishable as operators infect networks and gather information necessary to craft an attack. In these phases, even if the target detects the malware present in its assets, it is very difficult to assess motive and intent. Only once offensive modules are deployed can confidence in hostile intent increase. This adds an unfortunate layer of political nuance, as overly successful network intrusions may be misconstrued by the target as unduly aggressive. The risk of potentially undesired escalation has been aptly covered by Buchanan when discussing the "cybersecurity dilemma" (Buchanan 2017), an application of the classic security dilemma to network intrusions between nations.

Presence-based operations can potentially be high-risk, high-reward capabilities. Successfully pre-positioning assets in military or otherwise critical networks may potentially have meaningful impact on the course of conflict if used to facilitate strategic surprise or large-scale reduction in enemy capacity to operate. At the same time, presence-based operations are notoriously brittle, and their discovery can undo years of focused labor. By nature, such operations require tight, intensive, unyielding support of friendly intelligence assets to map the threat, generate initial persistent access, and successfully maneuver through complex tangles of military networks until the right targets are found. It is therefore understandable why these campaigns are often spearheaded by intelligence agencies with core expertise on network intrusions rather than deployed military forces.

The Lockheed-Martin F-35 Lightning II fighter aircraft is a fascinating example of a platform potentially vulnerable to both presence-based and event-based attacks. After two decades of development, the aircraft had started active deployment accompanied by a host of issues with its onboard software. These included major in-flight failures of the radar system (Gallagher 2016), issues with its onboard avionics (US DoD 2016, 35), and "…276 deficiencies in combat performance [designated] as 'critical to correct'…" (US DoD 2017, 48). Additionally, both the onboard systems and the logistical software used to manage the F-35 have demonstrated numerous vulnerabilities during security testing procedures, many yet to be addressed as of 2017 (US DoD 2017, 103–4). While onboard systems are unlikely to be directly connected to the internet (Lin 2010, 66), targeting one or more of the F-35's prized array of sensory inputs and communication methods is possible for a knowledgeable adversary.

12 These vulnerabilities do indeed exist, see for example US DoD (2017, 3).

An event-based attack might try to overwhelm or otherwise compromise some of the F-35's tactical data links, used to share data with allied assets in the air and on the ground. For compatibility purposes, this communication commonly occurs via the Link-16 protocol, an encrypted legacy protocol used by NATO forces since 1975. While it has undoubtedly undergone improvements over its lifecycle, the limitations in encrypting reliable airborne tactical traffic and the vast array of opportunities for US adversaries to intercept, analyze and exploit Link-16 protocol vulnerabilities raise the option that it may be compromised during an attack. Link-16 includes targeting information, location of friendly forces and directives from command forces (Hura et al. 2000). Interestingly, even oversight reports have indicated some issues with the Link-16 data that forced pilots to revert to voice communication (US DoD 2017, 70). Others have indicated intermittent problems with the Multifunction Advanced Data Link (MADL) system used to communicate between fifth generation stealth aircraft,[13] causing pilots to 'lose tactical battlefield awareness' (US DoD 2017, 71). Successfully compromising the F-35's data links is thus not unfeasible and may severely degrade aircraft battlefield performance.

The effects phase in this particular instance could include one of several options. As an example, a manipulation attack could alter the pilot's perception of the battlefield by adding, removing, or moving specific targeting points fed to the radar subsystem by external channels. A disruptive attack could try to overwhelm sensory input or prevent the aircraft from awareness of being acquired by a ground-based air-defense battery. The effects would thus be nearly instantaneous, limited in scope to the targeted aircraft, and tactical in nature.

A presence-based attack against the F-35 could take months to prepare, culminating in an elaborate effects phase saved for evoking strategic surprise or in dire need. Rather than targeting a single aircraft or sortie, attackers would instead target the peripheral networks that interface with the F-35 during its operational life cycle. These could be on-base networks, maintenance forces or third-party software providers. By doing so, an adversary may temporarily degrade or completely disable a large number of aircraft.

One supposed innovation in the F-35's software is the Autonomic Logistic Information System, or ALIS. With one ALIS station present at each unit operating F-35s, it allows semi-automated fleet management, mission management, logistics, and maintenance (Lockheed Martin 2009). As with other parts of the Joint Strike Fighter program, ALIS has been plagued with critical faults which are instructive in two relevant aspects: how ALIS might be vulnerable to presence-based operations; and how exploiting these vulnerabilities could lead to a strategic advantage when triggered in the effects phase.

13 Currently for the US, the F-22 and the F-35.

The issues in ALIS are varied. Attempts to deploy it in test environments have forced support personnel to lower network security settings to allow users to log on (US DoD 2017, 96). Incorrectly handled maintenance data has resulted in one instance in "major damage to a weapons bay door" (US DoD 2017, 96) from an incorrectly loaded bomb that got loose and struck the aircraft. In June 2017, a software error in ALIS grounded an entire F-35 unit until the issue was addressed (Freedberg Jr. 2017). It would therefore seem that the system can both be a boon to aircraft operators and an attack vector for offensive network operators. A single warfighting platform now presents a diverse, varied attack surface that can potentially be exploited during wartime.

All military offensive network operations can be a tremendous boon to military objectives across all levels of operation. Each type has unique characteristics, requires different support staff, and may weave into doctrine at varying locations. Where event-based operations may assist in crippling a local adversary network to facilitate joint strikes, a well-placed presence-based capability may sufficiently delay adversary decision-making and resource martialing to strategically diminish the capacity for effective response. From sowing tactical chaos to deceiving a carrier strike group, the potential is vast – if each category is understood, respected, and contextually integrated.

REFERENCES

Ablon, Lillian. 2017. Zero days, thousands of nights: the life and times of zero-day vulnerabilities and their exploits. Santa Monica: Rand Corporation.

Army Headquarters. 2003. "US Army Field Manual 3-13 - Information Operations."

Atkin, Thomas, James McLaughlin, and Charles Moore. June 26, 2016. Hearing Before the House Armed Service Committee. Washington DC. http://docs.house.gov/meetings/AS/AS00/20160622/105099/HHRG-114-AS00-Wstate-AtkinT-20160622.pdf.

Barrett, Neil. 2003. "Penetration Testing and Social Engineering: Hacking the Weakest Link." *Information Security Technical Report* 8 (4): 56–64.

Boyd, John. 1995. "The Essence of Winning and Losing." June 28. http://pogoarchives.org/m/dni/john_boyd_compendium/essence_of_winning_losing.pdf.

Bronk, Christopher, and Eneken Tikk-Ringas. 2013. "The Cyber Attack on Saudi Aramco." *Survival* 55 (2): 81–96. https://doi.org/10.1080/00396338.2013.784468.

Buchanan, Ben. 2017. *The Cybersecurity Dilemma Hacking, Trust and Fear Between Nations*. Oxford: Oxford University Press.

Burbank, Jack L., Philip F. Chimento, Brian K. Haberman, and William T. Kasch. 2006. "Key Challenges of Military Tactical Networking and the Elusive Promise of MANET Technology." *IEEE Communications Magazine* 44 (11). http://ieeexplore.ieee.org/abstract/document/4014472/.

Caltagirone, Sergio, Andrew Pendergast, and Christopher Betz. 2013. "The Diamond Model of Intrusion Analysis." DTIC Document. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA586960.

Chairman of the Joint Chiefs of Staff. 2006. "National Military Strategy for Cyberspace Operations."

Clarke, Richard A. 2009. "War from Cyberspace." *The National Interest*, 31–36.

Clausewitz, Carl Von. 1873. *On War*. 3rd ed. Vol. 1. London: N. Trubner & Co.

Coile, Gregory. 2009. "WIN-T SATCOM Overview Briefing." Program Executive Office Command Control Communications-Tactical. http://www.afcea-aberdeen.org/files/presentations/afceaaberdeen_ltccoile_28may2013.pdf.

Conti, Gregory, and David Raymond. 2017. *On Cyber: Towards an Operational Art for Cyber Conflict*. Kopidion Press.

Crawford, Bruce T., James J. Mingus, and Gary P. Martin. 2017. The United States Army Network Modernization Strategy. http://docs.house.gov/meetings/AS/AS25/20170927/106451/HHRG-115-AS25-Wstate-CrawfordB-20170927.pdf.

Dragos. 2017. "CRASHOVERRIDE: Threat to the Electric Grid Operations." Dragos. https://dragos.com/blog/crashoverride/CrashOverride-01.pdf.

Ducheine, Paul, and Jelle van Haaster. 2014. "Fighting Power, Targeting and Cyber Operations." In *Cyber Conflict (CyCon 2014), 2014 6th International Conference On*, 303–327. IEEE. http://ieeexplore.ieee.org/abstract/document/6916410/.

Epperson, Lynn. 2014. "Satellite Communications Within the Army's WIN-T Architecture" Program Executive Office Command Control Communications-Tactical. http://studylib.net/doc/18136899/satellite-communications-within-the-army-s-win.

Falliere, Nicolas, Liam O Murchu, and Eric Chien. 2011. "W32.Stuxnet Dossier" Symantec. https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

Farwell, James P., and Rafal Rohozinski. 2011. "Stuxnet and the Future of Cyber War." *Survival* 53 (1): 23–40. https://doi.org/10.1080/00396338.2011.555586.

Freedberg Jr., Sydney J. 2017. "ALIS Glitch Grounds Marine F-35Bs." *Breaking Defense* (blog). June 22, 2017. http://breakingdefense.com/2017/06/breaking-alis-glitch-grounds-marine-f-35bs/.

Gallagher, Sean. 2016. "F-35 Radar System Has Bug That Requires Hard Reboot in Flight." *Ars Technica*. March 10, 2016. https://arstechnica.com/information-technology/2016/03/f-35-radar-system-has-bug-that-requires-hard-reboot-in-flight/.

GCHQ. 2012. "Full-Spectrum Cyber Effects". https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH8311.dir/doc.pdf.

Giannangeli, Marco. 2017. "Russians 'Hacking into' RAF Crews over Syria." *The Daily Express*. January 15, 2017. http://www.express.co.uk/news/world/754236/russia-raf-bombers-syria-hacking-missions-military-army.

Hamill, Jasper. 2014. "Bank-Busting Jihadi Botnet Comes Back To Life. But Who Is Controlling It This Time?" *Forbes*. June 30, 2014. https://www.forbes.com/sites/jasperhamill/2014/06/30/bank-busting-jihadi-botnet-comes-back-to-life-but-who-is-controlling-it-this-time/#3df4bb0f6f07.

Hura, Myron, Gary McLeod, James Schneider, Daniel Gonzales, Daniel M. Norton, Jody Jacobs, Kevin M. O'Connel, William Little, Richard Mesic, and Lewis Jamison. 2000. "Tactical Data Links." In *Interoperability: A Continuing Challenge*, 107–21. Chapter 9 - Tactical Data Links: RAND.

Hutchins, Eric M., Michael J. Cloppert, and Rohan M. Amin. 2011. “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.” *Leading Issues in Information Warfare & Security Research* 1: 80.

Kaspersky Lab. 2014. “The Regin Platform: Nation State Ownage of GSM Networks” https://securelist.com/files/2014/11/Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf.

Kimmons, Sean. 2017. “Cyber Teams Throw Virtual Effects, Defend Networks against ISIS.” United States Army. February 15, 2017. http://www.army.mil/article/182400/cyber_teams_throw_virtual_effects_defend_networks_against_isil.

Langner, Ralph. 2011. “Stuxnet - Dissecting a Cyberwarfare Weapon.” *IEEE Security and Privacy* 9 (3): 49–51.

Libicki, Martin C. 2009. *Cyberdeterrence and Cyberwar.* Santa Monica, CA: RAND.

Lin, Herbert S. 2010. “Offensive Cyber Operations and the Use of Force.” *Journal of National Security Law and Policy* 4: 63.

Lockheed Martin. 2009. “Autonomic Logistics Information System (ALIS).” Lockheed Martin.

Malone, Jeff. 2010. “Intelligence Support Requirements for Offensive CNO.” presented at the Cyber Warfare and Nation States Conference, Canberra, Australia, August 23.

Monte, Matthew. 2015. *Network Attacks & Exploitation: A Framework*. Indianapolis, IN, USA: John Wiley & Sons, Inc. https://doi.org/10.1002/9781119183440.

NIST. 2017. “NVD - CVSS Severity Distribution Over Time.” NIST. 2017. https://nvd.nist.gov/vuln-metrics/visualizations/cvss-severity-distribution-over-time.

NSA. “Computer Network Operations - GENIE.” 2013. National Security Agency. https://www.eff.org/files/2015/02/03/20150117-spiegel-excerpt_from_the_secret_nsa_budget_on_computer_network_operations_-_code_word_genie.pdf.

Nye, Joseph S. 2010. “Cyber Power.” DTIC Document. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA522626.

Perlroth, Nicole, Mark Scott, and Sheera Frenkel. 2017. “Cyberattack Hits Ukraine Then Spreads Internationally.” *The New York Times*, June 27, 2017, sec. Technology. https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html.

Peterson, Dale. 2013. “Offensive Cyber Weapons: Construction, Development, and Employment.” *Journal of Strategic Studies* 36 (1): 120–24. https://doi.org/10.1080/01402390.2012.742014.

Rattray, Gregory J. 2001. *Strategic Warfare in Cyberspace*. Cambridge, Mass: MIT Press.

Rattray, Gregory J., and Jason Healey. 2010. “Categorizing and Understanding Offensive Cyber Capabilities and Their Use.” In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*. Washington D.C.: National Academic Press.

Rosenbach, Marcel, Hilmar Schmundt, and Christian Stöcker. 2015. “Source Code Similarities: Experts Unmask ‘Regin’ Trojan as NSA Tool.” *Spiegel Online*, January 27, 2015, sec. International. http://www.spiegel.de/international/world/regin-malware-unmasked-as-nsa-tool-after-spiegel-publishes-source-code-a-1015255.html.

Samit, Sarkar. 2016. “Massive DDoS Attack Affecting PSN, Some Xbox Live Apps.” Polygon. October 21, 2016. https://www.polygon.com/2016/10/21/13361014/psn-xbox-live-down-ddos-attack-dyn.

Symantec. 2017. “Internet Security Threat Report.” Symantec. https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf.

US Army. 2014. “Army Field Manual 3-38 - Cyber Electromagnetic Activities.”

US DNI. 2013. “A Common Cyber Threat Framework: A Foundation for Communication.” Office of the Direction of National Intelligence. https://www.dni.gov/files/ODNI/documents/features/Threat_Framework_A_Foundation_for_Communication.pdf.

US DNI. 2013. “Cyber Threat Framework Lexicon.” Office of the Director of National Intelligence.

US DoD. 5/17. “Joint Publication 1-02: DoD Dictionary.” US Department of Defense.

US DoD. 2003. “Information Operations Roadmap.” US Department of Defense.

US DoD. 2013. “Joint Publication 2-0: Joint Intelligence.” US Department of Defense.

US DoD. 2016. “Fiscal Year 2015 DoD Programs - F-35 Joint Strike Fighter (JSF).” US Department of Defense.

US DoD. 2017. “Aegis Modernization Report Program - Fiscal Year 2016.” US Department of Defense.

US DoD. 2017. “Fiscal Year 2016 DoD Programs - F-35 Joint Strike Fighter (JSF).” US Department of Defense.

US Joint Chief of Staff. 2013. “Joint Publication 3-12: Cyber Operations.” US Joint Chief of Staff.

US Press Secretary. 2018. “Statement from the Press Secretary.” The White House. February 15, 2018. https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/.

Wikileaks. 2017. “Vault 7: CIA Hacking Tools Revealed.” Wikileaks. March 7, 2017. https://wikileaks.org/ciav7p1/.