Noisy Operations on the Silent Battlefield

Preparing for adversary use of unintrusive precision cyber weapons

Forrest Hare | William Diehl

ABSTRACT

Cyber weapons can be divided into intrusive and unintrusive capabilities. Intrusive attacks, which require first gaining privileged access, have earned notoriety in the popular media. However, unintrusive attacks, which can be "noisy" but do not require privileged access, offer a potential cyber adversary many benefits. Using attack methods such as denial of service and telephony denial of service, and energy depletion attacks such as denial of sleep, an adversary can achieve demonstrable effects against a range of targets. These effects can be achieved while reducing the costly burden of pre-attack intelligence-gathering and pre-positioning of exploits that could signal intent or constitute a hostile act. The growth of the Internet of Things in national civilian and defense sectors has resulted in an expanded cyber-attack surface and increased the vulnerability of critical systems to certain unintrusive attacks. In this paper, we define, characterize, and present examples of unintrusive precision cyber weapons used in real-world operations. Given the high likelihood of encountering adversary employment of electronic warfare-like unintrusive capabilities, analyses of cyber conflict and friendly cyber security measures designed to defend against them should be predicated on scenarios that include their employment. Therefore, taking lessons from electronic protection doctrine, we advocate for preparation against the use of unintrusive precision cyber weapons through improved acquisition, training, and integration.

INTRODUCTION

In an insightful article on cyber warfare, "The Ethics of Cyberwarfare," Dipert divides offensive cyber weapons between those that conduct intrusive attacks, in which weapons gain unauthorized access to the functionality of a targeted system by first achieving privileged access, and unintrusive attacks, in which weapons achieve the desired effects through cyberspace without having privileged access to the targeted system.[1] Most research has focused on the challenges, ethics, and other strategic and tactical implications of intrusive attacks. For example, Libicki's analysis of *sub rosa* warfare is predicated explicitly on intrusive attacks, and Herr and Rosenzweig assess export control challenges based on their model of a cyber weapon that contains an exploit used specifically to gain access to a closed system.[2] However, academia and the popular media have focused less on the use of unintrusive attack methods that have been and could again be employed by adversaries during a conflict. Equally important are the implications of such attacks for the cyber defender responding to them. We argue that in future conflicts, potential adversaries will increasingly employ unintrusive precision cyber weapons (UPCW), which are similar to and facilitated by electronic warfare (EW) capabilities, in that they are both "noisy" and overt. This assertion is premised on several factors, such as the fact that UPCWs require less aggressive and less costly intelligence and can be employed in more diverse situations with a higher level of confidence in their effectiveness than intrusive weapons.

Based on Dipert's classification, we begin with a description of the two classes of offensive cyber capabilities and examples of types of attacks. We then review a selection of previous conflicts where unintrusive cyber weapons were operationally effective and discuss the benefits and challenges of choosing such capabilities over intrusive cyber weapons. Given the high likelihood of encountering adversary employment of UPCWs, potentially integrated with EW capabilities, we further argue that analyses of cyber conflict, and friendly cyber security measures to defend against them, should be predicated on scenarios that include their employment. Based on this assertion, we conclude by recommending where cyber defense measures could be more closely integrated with electronic protect measures.

Intrusive vs. Unintrusive Precision Cyber Weapons

In Dipert's taxonomy, cyber weapons can be divided into intrusive and unintrusive capabilities. Most academic research and popular press reports focus heavily on so-called intrusive cyber attacks, in which an aggressor, be it hobby-hacker, cyber criminal, or nation-state actor, gains some level of privileged access to computer programs, software, or stored data.[3] Using this class of cyber weapon, the attacker must act from inside the target system; they gain privileged access by using malicious software (malware) to manipulate the target system. Intrusive attacks can be labeled quiet, in that the attackers make a significant effort to remain undetected and leave no noticeable indicators of activity until the payload is activated; the attacker needs another software component or payload to achieve the desired effect against the targeted system during a conflict or contingency. The intrusive cyber weapon might also have a command-and-control entity that could be used to execute the entire operation. However, the attacker might never be able to assess battle damage inflicted on the targeted system, due to a lack of observable external effects.

Cyber-criminal organizations, hacktivists, and purported nation-state actors have conducted well-known intrusive cyber attacks during recent conflicts that required pre-positioned exploits. For example, Russia has been conducting a sustained but undeclared cyber war against Ukraine's military and civilian infrastructure for several years. In December 2015 and again in December 2016, Russia-associated actors attacked Ukraine's financial system, transport, and energy facilities using TeleBots and BlackEnergy malware.[4] These attacks required privileged access, which Russia gained over the course of six months as malware was downloaded to network systems. The attackers then used network access in energy company computers to pivot to supervisory control and data acquisition (SCADA) devices. When the time came to launch an attack, the actors remotely accessed the control devices and simply shut down the power. In one such event, up to 225,000 people were without power for several hours.[5]

The attack on the Ukrainian power system began by pre-positioning malware in the targeted systems, which required long-duration cyber reconnaissance that included computer network exploitation (CNE), target development, and network mapping. As we discuss later, such pre-positioned cyber exploits are ephemeral in nature; they can be neutralized, wittingly or unwittingly, by changes in network topology, by rerouting external communication links, or by improved cyber hygiene measures taken by the target organization. Moreover, a presumption of hostility or undeclared aggression either exists or is implied by conducting the cyber exploitation necessary to prepare intrusive attacks on sensitive national systems.

In contrast, an unintrusive precision cyber weapon employs techniques that do not require the attacker to first gain privileged access to achieve an effect on a desired target or to exploit correctable system vulnerabilities. Instead, a targeted device, which could be a node, server, sensor, actuator, or network, is disrupted or degraded so that it cannot function properly for a specific amount of time but is not otherwise permanently damaged; the effects of the attack begin on command and should stop when the attacker stimulus is removed. UPCWs are inherently noisy, in that their application is readily observable to attacker, victim, and third parties. The term "precision" as relates to these weapons refers to both time and space; in other words, the desired effects are achieved against a specific device, with limited collateral impact to non-targeted devices through random self-replication.

Although a potential attacker must understand the general technology of a targeted device, which could require intelligence preparation, research, and engineering capabilities, employing a UPCW requires only limited understanding of the target's specific configuration or of target details that cannot be gained through open sources, such as Internet-facing IP addresses. Moreover, their employment does not require *a priori* insertion of malware or Trojans; rather, the attacks are directed at general properties of the targeted device in conjunction with delivering effects. UPCW capabilities include Denial of Service (DoS) and Distributed Denial of Service (DDoS), Telephony Denial of Service (TDoS), and emerging cyber threats germane to the Internet of Things (IoT), including Denial of Sleep (DoSL).

In DoS and DDoS attacks, the attacker seldom gains privileged access to the target system. They instead often attempt to overwhelm a victim with legitimate or nearly legitimate service requests using normal network communications. DoS and DDoS are remarkably simple but successful attack vehicles, since networked target devices must service client requests in order to function. Typically, no physical or logical damage to target networks occurs; networks are simply denied or degraded for the duration of the attack. One must note, however, that DoS and DDoS attacks are often preceded by a lengthy period of acquiring botnets, which are third-party computing platforms that are maliciously coopted by an attacker, often by intrusive means such as implanting malware. The *a priori* coopting of botnets or other “zombie” devices is not required by an actor with sufficient means to provide its own attacking devices. However, a diverse set of unwitting third-party computing platforms provides topological separation of attack vectors, which makes it more difficult for a defender to use countermeasures (e.g., blocking attacks) while allowing legitimate requests. Cyber preparation of the battlespace to conduct DoS or DDoS is otherwise not difficult, given that most target devices are designed to be easily discoverable and reachable using highly standardized protocols.

In TDoS, an attacker disrupts telephone or associated communication services by initiating an overwhelming number of calls that prevent legitimate users from making calls during the attack; this move can be sustained as long as the attacker wishes to disrupt the targeted phone network. This kind of attack also can be used to support fraudulent activity, for example, by preventing a client from contacting their bank to verify a credit card transaction. Voice over Internet Protocol (VoIP) has made TDoS attacks more dangerous, including those on the legacy public switched telephone network (PSTN). The PSTN was formerly a closed system, is now integrated with IP packets, making attacks easier at the application level. Social media also can be used to initiate mass calling campaigns, as spoofed or anonymous calls are easier to make using these platforms.[6] As with DoS and DDoS, the intelligence preparations required to employ TDoS are generally not difficult, as many telephone numbers are publicly available, but even where they are not, the easy placement of telephony surveillance devices by cyber criminals and potentially by nation-state actors, such as international mobile subscriber identity catchers, greatly increases the potential for such attacks.[7]

The onset of new edge-computing enabled through the IoT has greatly expanded cyber-attack surfaces, in particular new attack vectors for unintrusive attacks. Attack surfaces have expanded due to three factors: (1) the sheer number and ubiquity of IoT devices, estimated to reach 24 billion out of 34 billion total Internet-registered devices by 2020; estimates are that 70% will have software vulnerabilities;[8] (2) low-cost and low-security devices, necessitated by a market model with a very low profit margin;[9] and (3) new attack vectors that can be used to inject, spread, and direct attacks through non-Internet connections, such as radio frequency, optical, or near field magnetic communication. All of these vectors facilitate attack propagation, even between and among air-gapped systems.[10]

IoT vulnerability to UPCW attacks was demonstrated during the October 2016 Dyn cyber-attack.[11] Mirai malware was installed on millions of IoT devices (e.g., web cameras, baby monitors, residential gateways), which overwhelmed the Dyn domain name server with resolution requests and took down large segments of the internet in Europe and North America. Future attacks of this type are increasingly likely to occur with IoT devices, since their low cost and low security standards often result in continued post-purchase use of default credentials.

Another class of UPCW has been made possible by the development and field deployment of IoT devices that often are not connected to electric power sources, relying instead, for example, on AA or 9V batteries. This configuration allows for unintrusive energy depletion attacks that are enabled by attempting to contact target devices using protocols that have varying degrees of legitimacy, which causes them to increase their processing power. Energy depletion attacks can be caused by simple wideband jamming designed to increase the noise environment, and they can cause IoT devices to use more power to transmit.[12] Attacks of this nature, such as DoSL attacks, can also be more sophisticated.

One well-studied example of a field-deployed IoT device is the wireless sensor network (WSN), which often consists of a simple processing core, such as a microcontroller, and uses a wireless radio standard to transmit environmental or sensor information to a central collector. Most contemporary microcontrollers have a low-power mode, which turns off the central processor and high-frequency clock and then enters sleep mode to preserve battery power during long-term independent operation. In one study, a WSN device was shown to consume up to 400 times more power in receive mode than in sleep mode, and up to 1,000 times more power in transmit mode than sleep mode.[13] Accordingly, using two standard 3000-mAh AA batteries, it can last 3,300 days in sleep mode but only 5.8 days in receive mode. The study also identified that energy wasted through collisions, control packet overhead, overhearing (i.e., being in receive mode while another node is transmitting), and idle listening (i.e., listening to unnecessary traffic in receive mode) can quickly drain the power of these WSN devices and render them inoperative.

Another type of attack is to target power consumption, which relies on power consumed during authentication. In an age where an adversary could attempt a masquerade, replay, or “man-in-the-middle” attacks, IoT networks need authentication protocols when a new node attempts to join a network through a wired or wireless connection. When devices are in sleep mode, requests to authenticate new devices cause them to enter processing modes, which vastly increases energy consumption.[14] Energy depletion is exacerbated by the challenges of authentication protocols, whose encrypted data streams can contain thousands of symbols.[16] To reduce processing and energy resources, IoT devices often use symmetric encryption (i.e., secret key cryptography) for authentication protocols. In symmetric encryption, both parties have the same secret key, which is usually short. For example, the current U.S. Advanced Encryption Standard and commercial encryption innovations such as Google Adiantum use

128-bit secret keys.[16] However, key distribution is challenging, which is one reason why IoT devices retain their factory settings that usually cannot be changed.

In contrast, in asymmetric encryption (i.e., public key cryptography), keys exist in pairs of public and private keys, and only one entity has the private key of a given public-private pair. Authentication is facilitated by asymmetric encryption, since only a known entity could feasibly respond with the correct private key. Public key cryptography requires orders of magnitude more processing power and much longer public keys (e.g., 256 bits for a current ECC algorithm and 3,072 bits for a current RSA algorithm. Increased use of processing and transmission power results in higher costs for commoditized IoT devices, which in turn results in the industry opting for cheaper but less secure solutions. DoSL attacks enabled by authenticating public key encryption will become more powerful in the next five to ten years, as designers are forced to incorporate post-quantum-resistant public key infrastructure, for which keys could be tenfold longer than current and projected public and private key lengths.[17]

To summarize, the operational concept of energy depletion attacks, forcing devices to wake repeatedly from sleep mode, to increase processing or transmission power in order to carry out their mission, an adversary need only study IoT network protocols and bombard target networks with traffic that has various degrees of illegitimate or nearly legitimate packets.

Examples of UPCW Usage in Regional Conflicts

The use of UPCW in operational scenarios and as a means to achieve state objectives is not far-fetched; it has been demonstrated on several occasions. In 2007, alleged Russian “patriotic hackers” launched a DDoS attack against Estonia, due to Estonia’s plans to remove World War II monuments honoring the Russians.[18] These attacks were focused on disrupting government institutions and disabling commerce. The cyber attacks, however, were not followed by or coordinated with kinetic military operations, since aggression against a NATO member was either beyond the limits of Russia’s strategic risk or objectives at the time. The use of non-governmental agents gave the Russian government plausible deniability while successfully sending a message to their much smaller neighbor about how vulnerable it would be in a conventional fight.

By August 2008, the Russians had begun to combine cyber and kinetic operations in their brief conflict with Georgia. Russia conducted DDoS attacks against Georgian internal communications; cyber operations were coordinated with military operations as part of the Russian response to Georgian military operations in the breakaway Georgian regions of Abkhazia and South Ossetia. This was arguably the first coordinated use of military and network-based cyber operations as part of a synchronized strategy.[19] These attacks were intended to deny, disrupt, and affect the overall flow of information inside Georgia by overloading government sites with requests and disrupting telecommunications nationwide. The attacks did not require exploits to be implanted in advance in the target machines as they used thousands of previously co-opted zombie bots to send requests. These DDoS also employed structured query language (SQL) injections/cross-site scripting (XSS), which can be used to deny services. Public email addresses were also utilized for psychological operations. These various attacks were ostensibly attributed to Russian "cyber militia" instead of official Russian government.

By 2014, the Russians had honed unintrusive (but noisy and disruptive) cyber operations down to a finely tuned science. They turned to lower technology methods to launch coordinated cyber attacks that disrupted Ukrainian government functions while pro-Russian rebels seized Crimea in March 2014. They simultaneously sowed the seeds of malware exploits for future intrusive cyber operations. The operations against Ukraine consisted of TDoS attacks on mobile phones, which originated in Crimea.[20] The attackers used equipment installed in the Ukrtelecom networks in the Crimea region under control of Russian forces. However, DDoS attacks on most web services in Crimea were not required by cyber means, as many already were under the physical control of Russian forces by the start of the conflict; in short, the occupying forces simply turned off the servers.

The current and coming increased use of UPCW by Russia in combat scenarios portends closer integration of cyber and EW capabilities, as EW platforms are well-suited to deliver synchronized effects across the multiple attack surfaces utilized by modern IT devices. As a powerful example, Russian cyber operations have been, and are poised to get, much noisier than legacy DoS attacks. Over the last 10 years, they have developed, fielded, and employed battlefield EW capabilities with impunity and are now able to affect cyber conditions at the operational level through integrated platforms. One such example is Russian use of the R-330ZH Zhitel. The R-330ZH conducts barrage noise jamming of tactical radio nets, cell phone emitters, and satellite downlink targets, and it can locally nullify communications and GPS signals. It is designed for detection, analysis, direction-finding and jamming satellite and cellular phone communication systems operated in the frequency from 100 to 2,000 MHz. Effects of the R-330ZH as a battlefield EW system are clearly observable to targeted systems; it is noisy and overt, and the degradation of communications networks ceases when jamming ceases.[21]

At this point, we have defined and characterized UPCW, discussed the types of attacks where their use might be effective, and reviewed real-world operational scenarios in which UPCW-type weapons were employed. Given this background, we can now discuss the benefits of such weapons to a potential cyber aggressor and why they likely will be employed in future conflicts.

Potential Benefits of Developing and Employing UPCW

The cyber belligerent will enjoy several potential benefits when integrating UPCW with conventional military operations. The first benefit is a reduced need for high-fidelity and difficult-to-gather target intelligence when developing and employing advanced cyber weapons. While an adversary must still invest in research and development against target-specific capabilities, the *a priori* insertion of fragile malware or Trojans into target networks is not required; rather, the attacks are directed at general properties of the targeted device in conjunction with delivering effects. This benefit can be contrasted with the intelligence requirements for intrusive cyber weapons. Each component of an intrusive cyber weapon system requires specific intelligence; the more complex the capability, the more complex the intelligence required. For example, a capability that employs an intrusion exploit, a remote command-and-control mechanism, the ability to elevate privileges and move laterally in a system without being detected, and a payload to achieve an effect on a specific component within the system requires exquisite intelligence for each component of the weapon. The operator needs to know software versions of the target systems, the target's network addresses, details of the cryptography employed by the defender and of the defenders' operational tactics to avoid being seen by them, and a host of other requirements. Even if the details for building an exquisite cyber weapon can be found on the Internet, the intelligence required to employ the weapon against a specific national security related target network must be gathered by an advanced intelligence organization. What complicates the intelligence requirements further is the fact that the intelligence details will change over time; for example, administrators, network configurations, and software will change. As a result, the intelligence must be constantly checked for accuracy, which requires additional intelligence missions that give the defender repeated chances to be tipped off to malicious activity on their networks.

These enormous intelligence requirements favor countries with advanced signals intelligence (SIGINT) and CNE capabilities.[22] However, an intelligence organization's ability to support the development of intrusive capabilities does not directly equate with a desire to support their development. Cyber operators will most likely have to compete with national foreign intelligence requirements to satisfy their cyber-development requirements. This would require them to make the case to their intelligence support units that the exquisite cyber weapon's future potential to support military operations outweighs the immediate benefit to leaders from acquiring foreign intelligence. Therefore, there likely would be significant pressure to develop capabilities requiring less detailed intelligence, even in countries with advanced intelligence capabilities. Countries without advanced SIGINT and CNE capabilities would have an incentive to employ UPCW, given that such capabilities would create fewer intelligence-related barriers to entering the cyber conflict. Focusing on UPCW would reduce the need to develop the skill sets and infrastructure required to obtain the highly detailed and perishable intelligence necessary to support employment of intrusive cyber weapons.

A second and directly related advantage is that an unintrusive precision cyber weapon's capability is less ephemeral and requires less technically skilled operators than an intrusive one's. As described by Smeets, cyber weapons are generally more transitory than conventional kinetic weapons because their "ability and effectiveness to cause harm declines relatively quickly."[23] For example, an offensive cyber capability often can be neutralized before it is used if a network defender upgrades its software or firmware, installs a patch, or changes passwords. The transitory nature of an intrusive cyber weapon is compounded by the fact that any change made by the defender, whether specifically to increase security or to restructure the domain, could create a formidable barrier to the attacker if they are unaware of the details of the change. A simple measure such as conducting an off-site backup may be sufficient to counter a complex attack. Changes to any component of the target system or its defenses could cause the overall capability of the attack to malfunction and reduce confidence in its ability to achieve effects when and where desired on command. To counteract these factors, would-be aggressors need skilled operators who can develop effective weapons quickly and test their effects against ever-morphing targets. UPCW, on the other hand, can be employed by operators with much less detailed training in their development and employment, as Russia demonstrated in the Georgia conflict.[24] This increases a military force's ability to train a large cadre of cyber operators, who can train with other combat forces directly in preparation for a conflict. With this consideration in mind, one would expect that, the less complex the cyber weapon, the less transitory it will be, and the greater the likelihood of achieving a return on investment in its development and employment. The potential return on investment would increase whenever the cyber defender further improved its cyber security posture or patched potential vulnerabilities against intrusive weapons.

A third advantage arises from the fact that unintrusive capabilities do not require advance emplacement of exploits that need monitoring, so there is less potential to signal intent before the weapon is employed during a conventional military operation. Even conducting reconnaissance before attempting to emplace an exploit could tip a defender to an attacker's intent if the reconnaissance is sufficiently aggressive. Without the need to maintain access to an exploit that has been inserted in an adversary's cyber system that required privileged access, the UPCW operator can more easily maintain positive command and control of the cyber weapon without any warning signals being broadcast to a target. This increases the chance that the attack can be initiated at the correct location and specified time to support conventional or other cyber operations. The increased precision possible when having direct command and control of the system increases a military commander's confidence in a cyber weapon's ability to support operations as needed. In addition, simplified and direct command and control of an unintrusive weapon should enable the operator to reverse effects more easily and rapidly. On the other hand, when an intrusive weapon is employed for which the attacker expects to lose direct command-and-control ability, the command to cease effects must be encoded in the payload, should that capability be desired. For example, if the "defuze" command is dependent on environmental conditions that could change if the target system software is upgraded, the command may never be delivered.

A related advantage that stems from delivering effects on the outward-facing components of the targeted system is that the cyber operator employing UPCW can measure the effectiveness of weapon employment more directly. When complex cyber weapons are employed that have effects on targets that are not directly observable—for example, disrupting a server within a closed network—the attacker might never be able to confirm the weapon's effectiveness. When employing unintrusive measures, the effects on the target are likely more accessible for a battle damage assessment and can be reported to other forces that are relying on the effects of the weapon to conduct their mission. The increased ability to measure the effectiveness of an attack increases both confidence in its use and the probability that a military commander will advocate to integrate the UPCW with conventional military operations.

These advantages cascade to create additional advantages. For example, the increased likelihood of using unintrusive cyber weapons will enable operators to learn from their use and improve their effectiveness. This advantage leads to a greater ability to exercise with the capability and to use UPCW multiple times during a conflict. This increased knowledge and efficacy will increase a commander's confidence in the future success of UPCW and have a self-promoting influence on their development. It appears, for example, that the Russians have learned from their experiences in Georgia and Ukraine, as we see their military commanders becoming more confident in the effectiveness of UPCW. Gen. Raymond Thomas, former commander of U.S. Special Forces Command, stated that Syria is the "most aggressive EW environment on the planet... They are testing us every day, knocking down our communications."[25]

Lastly, there is less pressure to "use it or lose it." Some authors argue that the transitory nature of intrusive cyber weapon systems increases the likelihood that they will be employed in a preemptive situation because they must be used before they become obsolete.[26] In fact, if the arguments we have made to this point support the notion that our adversaries are instead developing unintrusive capabilities, which we expect would have less devastating effects on our systems, we also can assume that it reduces the pressure for them to "use them or lose them." This would possibly reduce the pressure we feel to develop exquisite, intrusive cyber weapons to avoid losing a cyber arms race.

Challenges

Despite the benefits belligerents might gain by using UPCW in a conflict, they also will face challenges. First, noisy cyber weapons can more easily be attributed to an adversary. The noisier the attack, the more quickly the victim will begin tackling the attribution issue. A counterpoint would be that, given that these weapons would most likely be employed during an ongoing conventional military conflict, concern about attribution would most likely not influence the attacker's decision to employ them.[27] Even with the potential for attribution, it is difficult to identify the exact origin point of an attack, which creates plausible deniability for specific actors. Moreover, distributed attack surfaces, such as botnets, will obscure the identity of the sponsors of such attacks and increase the potential for plausible deniability.

Second, in any cyber campaign between nation-states, there is a tendency for technically capable, idealistic or nationalistic patriotic hackers to join the fray.[28] Patriotic hackers traditionally conduct noisy attacks and do so on purpose, as they want their presence to be felt. They also provide a convenient cover for a military if anonymity is still desired. However, for those who want to act according to the Law of Armed Conflict, the participation of patriotic hackers can lead to a loss of control of cyber actions, as the hackers cannot be controlled as readily as military forces. Therefore, they may not act with the desired precision in terms of the specified target and the duration of the attack. Limited effectiveness in Georgia and indiscriminate attacks on US and Estonian targets during these events caused unwanted problems for Russia.[29] As discussed by Gelb and Libicki, politicians often fear losing the war less than losing control of the war, therefore, weapons that cannot be controlled effectively by a central command structure are problematic if war is to be a "continuation of politics by other means."[30] However, nation-states that are reasonably confident in their ability to maintain control over their populace, including any accompanying internal information campaign, are less likely to be dissuaded by patriotic hackers and may actually exploit this phenomenon to their advantage.

Implications for the Defender

Given the benefits of developing less sophisticated UPCW, the implications for the cyber defender are clear—the defender must prepare for increased adversary use of UPCW, both in future conflicts involving integrated employment of kinetic and non-kinetic weapons, and in periods of heightened tensions where non-kinetic weapons can be used for strategic signaling and psychological effect. Increased cyber security spending in the U.S. Department of Defense, the stand-up of U.S. Cyber Command (USCYBERCOM), and the coordination of improved cyber security with critical infrastructure providers will continue to reduce our vulnerability to cyber weapons in general, and to complex weapons specifically. However, organizations charged with the research, development, and acquisition of cyberspace-dependent systems should clearly understand the vulnerabilities of complex command, control, communications, and intelligence (C3I) and UPCW combat systems, especially those enabled by flexible IoT devices.

Commanders also should consider the increased probability of early use of UPCW and adjust their training and defensive plans accordingly. Given the lessons learned from the employment of UPCW described above, UPCW are likely to be used not only against military C3I and combat systems, but against dual-use systems such as national telecommunications networks and power grids. Such systems support friendly military operations but also guarantee the security and well-being of civilian populations and friendly nations.

Furthermore, while this article takes no position on the merging of cyber and EW operations organizationally, it is clear that EW capabilities have been, are currently, and will be used in the future by potential adversaries to achieve integrated cyber effects. On a related note, the similar effects created by EW weapons and UPCW suggest that cyber defenders may learn from the EW community how to improve cyber defense. For example, Joint Electronic Warfare Doctrine describes the U.S. military's procedures for conducting frequency-management functions to ensure availability of the electromagnetic spectrum during a military operation.[31] Frequency management procedures establish critical requirements for frequency usage and outline coordination requirements with host-nation agencies. Perhaps the cyber defender could implement similar measures to ensure the availability of bandwidth via all mediums, to include RF, during a military operation. An additional electronic protect operation that might translate to defensive measures against UPCW attacks is Electromagnetic Interference (EMI) resolution. EMI resolution is a step-by-step process used to systematically diagnose the source or cause of EMI.[32] The same procedures could be employed to identify and counter the source of such attacks as TDoS, DDoS, and DoSL.

Finally, while our emphasis is on defense, friendly actors should consider investigating and developing improved UPCW options. This would help them understand the technology and operating characteristics of such weapons and give commanders symmetric response options in case of adversary use of UPCW. A symmetric response may provide options to deescalate a conflict in a manner more predictable than an asymmetric response option. As discussed in the recently published U.S. National Cyber Security Strategy, U.S. forces require response options to meet the mandate to employ military action in response to malicious cyber activities, both kinetic and cyber actions, in order to inflict swift and transparent consequences.[33] Furthermore, employment of UPCW could meet the USCYBERCOM priority for "persistent engagement" of contesting the adversary below the level of armed conflict.[34]

CONCLUSIONS

In this article, we have explored the less debated category of cyber weapons called unintrusive precision cyber weapons. We have argued that, although most academic research and sensational press are focused on intrusive cyber weapons that require exploits gained through privileged access, the relative advantages of unintrusive cyber weapons, including the lower bar of entry for a potential belligerent, merit increased consideration. This is especially relevant, given the last decade of increased cyber conflict between nation-state actors and the emergence of new technologies such as the IoT, which have exponentially expanded attack vectors and complicated a defender's task.

Of pressing concern to the defender are the magnified effects achieved by the integration of cyber and EW capabilities. US research, development, and acquisition organizations should carefully consider the increased attack surface afforded by the IoT and ubiquitous connectivity. The future use of UPCW, including combined cyber-EW attacks, should be studied during training and exercises and envisioned in tactical, operational, and strategic planning. Finally, the US should consider the study, development, test, and evaluation of UPCW capabilities in order to understand the challenges of this domain more fully, and to ensure the continuity of response options across the spectrum of kinetic and non-kinetic conflict.

Author Bios

Dr. Forrest Hare

Dr. Forrest Hare is a retired USAF Colonel currently serving as a Solution Architect for SAIC. As a major, he commanded an information warfare detachment in the European Air Operations Center during Operation Enduring Freedom. While assigned to Headquarters Air Force, Dr. Hare was chosen to be on the Chief's Cyberspace Task Force to develop the vision for the Service's operations in its newest warfighting domain. His work contributed to the stand-up of the 24th Air Force and new cyberspace doctrine. After this assignment, he served on the Secretary of Defense staff and was a drafter of DoD Cyber Security policy. Dr. Hare has also served at the National Security Agency and in numerous overseas postings and deployments. In his current position at SAIC, he is developing an ontology-based knowledge model for defense intelligence to improve the integration of cyber threat intelligence with traditional intelligence information.

Dr. William Diehl

Dr. William Diehl is an Assistant Professor in the Bradley Department of Electrical and Computer Engineering at Virginia Polytechnic Institute and State University (Virginia Tech), a member of the Center for Embedded Systems for Critical Applications (CESCA), and an affiliated faculty member of the Hume Center for National Security and Technology. His area of research is secure and efficient implementations of cryptographic algorithms in hardware and software, including field programmable gate arrays (FPGA), Systems-on-Chip (SoC), microcontrollers, and soft-core microprocessors. Dr. Diehl previously served in the U.S. Navy as a Surface Warfare Officer and Cryptologic Officer, and retired at the rank of Captain. Dr. Diehl completed his B. A. at Duke University, M.S. at the Naval Postgraduate School, Master's Degree in Strategic Studies at the Air War College, and Ph.D. at George Mason University.

NOTES

1. Randall R. Dipert, “The Ethics of Cyberwarfare,” *Journal of Military Ethics* 9, no. 4 (December 2010), 384–410, https://doi.org/10.1080/15027570.2010.536404.
2. Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007);Trey Herr and Paul Rosenzweig, “Cyber Weapons and Export Control: Incorporating Dual Use with the PrEP Model,” J*ournal of National Security Law and Policy* 8 (2016 2015), 301.
3. See, for example, Libicki, *Conquest in Cyberspace*; Herr and Rosenzweig, “Cyber Weapons and Export Control.”
4. Pavel Polityuk, “Ukraine Points Finger at Russian Security Services in Recent Cyber Attack,” *Reuters*, July 1, 2017, https://www.reuters.com/article/us-cyber-attack-ukraine-idUSKBN19M39P.
5. Polityuk, “Ukraine Points Finger.”
6. Rod Wallace, “The Surging Threat of Telephony Denial of Service Attacks,” Industry Report, San Antonio, TX: SecureLogix and Cisco, October 21, 2014.
7. Christopher Krebs, “DHS Response to Senator Ron Wyden,” Letter of Record from Acting Under Secretary, National Protection and Programs Directorate, March 26, 2018, https://www.documentcloud.org/documents/4429966-DHS-response-to-Wyden-3-26-18.html.
8. Finjan Team, “IoT DoS Attacks—How Hacked IoT Devices Can Lead to Massive DoS Attacks,” *Finjan Blog* (blog), August 20, 2018, https://blog.finjan.com/iot-dos-attacks/.
9. Vladimir Shakhov and Insoo Koo, “Depletion-of-Battery Attack: Specificity, Modelling and Analysis,” *Sensors* 18, no. 6 (June 2018): 1849, https://doi.org/10.3390/s18061849.
10. Eyal Ronen et al., “IoT Goes Nuclear: Creating a ZigBee Chain Reaction,” November 21, 2018, http://www.eyalro.net/project/iotworm/.
11. Dave Lewis, “The DDoS Attack against Dyn One Year Later,” *Forbes* (blog), October 23, 2017, https://www.forbes.com/sites/davelewis/2017/10/23/the-ddos-attack-against-dyn-one-year-later/.
12. V. A. Desnitsky, I. V. Kotenko, and N. N. Rudavin, “Protection Mechanisms against Energy Depletion Attacks in Cyber-Physical Systems,” in *IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering* (EIConRus), 2019, 214–19, https://doi.org/10.1109/EIConRus.2019.8656795; Shakhov and Koo, “Depletion-of-Battery Attack.”
13. D. R. Raymond et al., “Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols,” *IEEE Transactions on Vehicular Technology* 58, no. 1 (January 2009): 367–80, https://doi.org/10.1109/TVT.2008.921621.
14. C. Gehrmann, M. Tiloca, and R. Höglund, “SMACK: Short Message Authentication Check against Battery Exhaustion in the Internet of Things,” in 12th *Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, 2015, 274–82, https://doi.org/10.1109/SAHCN.2015.7338326.
15. Eduard Marin et al., “On the Feasibility of Cryptography for a Wireless Insulin Pump System,” in *Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy*, CODASPY ’16 (New York: ACM, 2016), 113–20, https://doi.org/10.1145/2857705.2857746.
16. Paul Crowley and Eric Biggers, “Adiantum: Length-Preserving Encryption for Entry-Level Processors,” *IACR Transactions on Symmetric Cryptology*, December 13, 2018, 39–61, https://doi.org/10.13154/tosc.v2018.i4.39-61.
17. Lily Chen et al., “Report on Post-Quantum Cryptography,” Gaithersburg, MD: National Institute of Standards and Technology, April 2016, https://doi.org/10.6028/NIST.IR.8105.
18. “A Cyber-Riot,” *Economist*, May 10, 2007.
19. “The Russo-Georgian War 2008: The Role of the Cyber Attacks in the Conflict” (white paper), AFCEA Cyber Committee, May 24, 2012, https://www.afcea.org/committees/cyber/documents/therusso-georgianwar2008.pdf.
20. “Crimea—The Russian Cyber Strategy to Hit Ukraine,” *Infosec Resources* (blog), March 11, 2014, https://resources.infosecinstitute.com/crimea-russian-cyber-strategy-hit-ukraine/.
21. Rob O’Gorman, “Intelligence Brief: Russia’s Electronic Warfare Capability in Ukraine,” *Open Briefing* (blog), July 7, 2015, https://www.openbriefing.org/publications/intelligence-briefings/russias-electronic-warfare-capability-in-ukraine/.
22. Max Smeets, “A Matter of Time: On the Transitory Nature of Cyberweapons,” *Journal of Strategic Studies* 41, nos. 1–2 (February 23, 2018), 6–32, https://doi.org/10.1080/01402390.2017.1288107.
23. Smeets, “A Matter of Time.”

NOTES

24. Jeffrey Carr, “Project Grey Goose Phase II Report” (Seattle: Grey Logic, March 20, 2009), fserror.com/pdf/GreyGoose2.pdf.
25. Colin Clark, “Russia Widens EW War, ‘Disabling’ EC-130s OR AC-130s In Syria,” *Breaking Defense* (blog), April 24, 2018, https://breakingdefense.com/2018/04/russia-widens-ew-war-disabling-ec-130s-in-syria/.
26. Andrew Krepinevich, “Cyber Warfare: A ‘Nuclear Option’?” Study on Future Warfare and Concepts, Center for Strategic and Budgetary Assessments, August 24, 2012, https://csbaonline.org/research/publications/cyber-warfare-a-nuclear-option.
27. Thomas Rid, “Cyber War Will Not Take Place,” *Journal of Strategic Studies* 35, no. 1 (2012): 5–32, https://doi.org/10.1080/01402390.2011.608939.
28. Forrest B. Hare, “Privateering in Cyberspace: Should Patriotic Hacking Be Promoted as National Policy?” *Asian Security* 15, no. 2 (May 4, 2019): 93–102, https://doi.org/10.1080/14799855.2017.1414803.
29. Azhar Unwala and Shaheen Ghori, “Brandishing the Cybered Bear: Information War and the Russia-Ukraine Conflict,” *Military Cyber Affairs* 1, no. 1 (December 16, 2015), http://dx.doi.org/10.5038/2378-0789.1.1.1001.
30. Martin C. Libicki, “Sub Rosa Cyber War,” in *The Virtual Battlefield: Perspectives on Cyber Warfare*, ed. Christian Czosseck and Kenneth Geers (Amsterdam: IOS Press, 2009); Leslie H. Gelb and Richard K. Betts, *The Irony of Vietnam: The System Worked*, Washington, DC: Brookings Institution Press, 2016; Carl von Clausewitz, *On War*, London: Kegan Paul, Trench, Trübner & Company, 1908.
31. “Joint Publication 3-13.1 Electronic Warfare,” Joint Staff, US Department of Defense, February 8, 2012.
32. “Joint Publication 3-13.1.”
33. “National Cyber Strategy of the United States of America,” Washington, DC: The White House, September 2018, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
34. C. Todd Lopez, “Persistent Engagement, Partnerships, Top Cybercom’s Priorities,” Government Document, U.S. Department of Defense, May 14, 2019, https://dod.defense.gov/News/Article/Article/1847823/persistent-engagement-partnerships-top-cybercoms-priorities/.