Information & Security: An International Journal

Arnold C. Dupuy, v.39:2, 2018, 163-174 https://doi.org/10.11610/isij.3914

CYBER-ENERGY INFRASTRUCTURE VULNERABILITIES IN THE HYBRID WARFARE ENVIRONMENT: SOME DOD MITIGATION EFFORTS

Arnold C. DUPUY

Abstract: The energy sector has long been recognized as critical infrastructure, particularly vulnerable to external penetration and manipulation by hostile elements. The cyber-energy nexus was chosen as the case study for this article. It highlights the growing vulnerabilities of the energy infrastructure to cyber threats and aims to move forward dialogue, mainly from the perspective of the US Department of Defense (DoD), on protecting DoD energy infrastructure from a variety of hybrid tools.

Keywords: critical infrastructure, hybrid warfare, non-linear warfare, cyber-energy nexus, operational energy context, joint mission assurance assessments, interagency, international cooperation.

Introduction

I was quite flattered when CAPT Yanakiev asked me to contribute to the International Conference on Interagency and International Cooperation in Countering Hybrid Threats in Sofia. Several years ago, I was invited to a conference organized by the G.S. Rakovski National Defense College's Defense Advanced Research Institute, so I was glad to contribute again. Though I'm unable to attend in person, I felt compelled to share my concerns as they relate to the topic, notably how cyber warfare has become a significant component to the hybrid warrior's arsenal. This becomes all the more dangerous when one considers the inherent vulnerabilities present in the energy sector.

To be clear upfront, this paper is neither a detailed analysis of hybrid warfare nor a technical evaluation of the broader cyber-energy fields. Also, it is not a comprehensive overview of all the Department of Defense's (DoD) efforts in cyber-energy defense. The purpose is to highlight and move forward dialogue into the growing vulnerabilities of the energy infrastructure to cyber threats, but mainly from a DoD con-

text. The cyber-energy nexus was chosen as the case study for this paper because energy, as a "uniquely" critical infrastructure, is particularly vulnerable to external penetration and manipulation by hostile elements.[1]

Identifying, responding to and recovering from cyber-attacks is a challenge, since it is difficult to separate the defense and civilian energy infrastructures. Nevertheless, there are clearly unique considerations that DoD, and all other defense establishments worldwide, must acknowledge; technological advances in telecommunications have created a host of new threats for the defense professional, threats that span both regular and irregular warfare. Indeed, the cyber threat transcends both the virtual (information technology) and physical (operational technology) realms, hence the emergence of a new field of analysis, 'hybrid warfare' as a way to identify and codify these new threats. For this very reason the topic resonates with this conference's primary goals which is to address interagency and international cooperation in this space. First, I felt it important to establish an intellectual foundation of hybrid warfare and what it constitutes.

What is Hybrid Warfare?

There is no formal definition of hybrid warfare. In its 2010 study, the U.S. Government Accountability Office (GAO) defined it as "…a blending of conventional and irregular approaches across the full spectrum of conflict."[2] Frank Hoffman in the blog, War on the Rocks, refers to it as "a tailored mix of conventional weapons, irregular tactics, terrorism, and criminal behavior in the same time and battlespace to obtain [a group's] political objectives."[3] In the May 2015 NATO Defense College Conference Report, hybrid warfare is defined as, "…the denial of—and defection from—standard norms and principles of international relations in pursuit of narrow interests, hybrid warfare in today's world is strategic in its ambition, and employs a mix of disinformation, destabilizing gambits and intimidation to force an adversary to comply with those interests." All with the goal of keeping an adversary "politically, militarily and societally off-balance."[4]

Quite often hybrid warfare has been referenced in conjunction with Russia or Islamic State as a tactic to circumvent Western operational countermeasures. Indeed, whether accurate or not, the genesis of hybrid warfare doctrine is traced to the February 2013 article by the Russian Chief of the General Staff, General Valery Gerasimov entitled, "The Value of Science in Prediction," which describes "non-linear warfare." This is believed to be the blueprint for Russian hybrid doctrine, and while the article is not so much a "doctrine," but acts as a rough outline of Gerasimov's thoughts, whereby one force applies concentrated power to the other's weak spots.

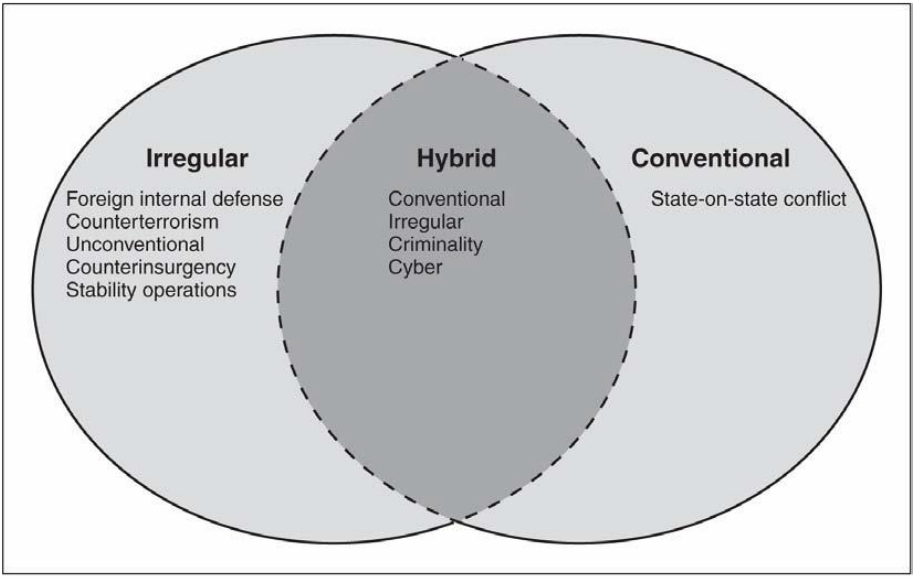
Figure 1: Valery Gerasimov, father of Russian hybrid warfare doctrine?

Yet, when analyzing the Russian example more closely, the results of hybrid warfare are somewhat mixed. Arguably, Russia's relative success in Crimea can be attributed to hybrid, or non-linear operations, however the deployment of special forces (aka "Little Green Men") with sanitized uniforms is hardly unique. More telling was the unprepared state of Ukraine's military and its inability to counteract any of the operational or political moves from the Kremlin. When looking at Moscow's efforts in the Donbas, what becomes clear is the hybrid component proved unsuccessful and only with the large-scale introduction of Russian conventional forces in August of 2014 did the situation stabilize in Moscow's favor. The result is in effect a new "frozen conflict" under Kremlin control.

Figure 2: Little Green Men, Crimea, 2014.

So, is hybrid warfare the latest buzzword put out by experts or is it truly a unique phenomenon? One can argue that hybrid warfare used to be called any number of terms in previous generations; irregular, unconventional, asymmetric, grey area, ambiguous, etc. In other words, humans have been leveraging their opponents' weaknesses since the beginning of time, using unconventional methods across the full political, military, social and economic fields. The idea is not to debate terminology, but recognize that changes are afoot in the security field. And though there may be a variety of definitions, hybrid warfare, as the name implies, is an ambiguous blend of regular and irregular warfare. This basic definition will act as the foundation for further discussion in this paper.

According to the GAO report, "DOD has not officially defined 'hybrid warfare' because DOD does not consider it a new form of warfare." However, DoD does use the term "hybrid" to describe the increasingly complex nature of conflict that will require adaptive and resilient responses. Indeed, "hybrid" and hybrid-related concepts are found in strategic planning documents, notably the 2010 Quadrennial Defense Review Report (QDR). That said, "hybrid warfare" has not been, and will not be incorporated into a doctrine, so the use of such terminology in official strategic documents is anomalous.



Source: GAO analysis of DOD military concept and briefing documents and academic writings.

It is hard to ignore that clear trends are appearing with an emphasis on lighter forces employing speed, stealth and agility, with information technology infused into the broader operational environment. Arguably, the only truly unique component of hybrid warfare is the cyber element, whereby virtual actions can have real-work consequences threatening life and property. While irregular warfare and its countermeasures are well-documented, with a variety of effective best practices in its implementation, the cyber component is still too new, with rapidly mutating technologies and leap-frogging offensive and defensive capabilities. This reliance on cyber assets is a relatively new component to communications and electronic warfare, which allows denial of service, the acquisition of intellectual property or secrets that such attacks can be conducted from a third-party location, which makes attribution difficult if not impossible.

The U.S. Department of Defense (DoD) Experience

The threats emanating from the cyber sphere have been the impetus for robust analysis within the U.S. Government. In DoD, the creation of U.S. Cyber Command in 2009 is perhaps one of the most visible aspects of addressing this threat, though all the Services have cyber defense efforts.[5] Nevertheless, the scale of the problem is growing with implications to national security. Broadly speaking, DoD spends hundreds of millions of dollars per year on cyber security for information systems (IS) and to mitigate the national security threats from millions of associated IS devices. Until fairly recently, cyber vulnerabilities were usually seen in the realm of information technology, such as documents or data repositories, which were subject to being hacked by external factions and the files extracted.

Existing in the IS sphere is Platform Information Technology (PIT), defined by Department of Defense Instruction (DODI 8500.01) as "…both hardware and software, that is *physically part of*, dedicated to, or essential in real time to the mission performance of special purpose systems."[6] Delving deeper into the PIT realm, Control Systems[7] (CS) are a subcomponent which encompass multiple physical systems, with direct applicability to the security of the operational energy infrastructure. Therefore, CS can be a critical enabler, which, when deployed on a network, provides vital support to dependent systems in command, control, communications and logistics. CS includes supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other systems such as Programmable Logic Controllers (PLCs), which are frequently used in industry and critical infrastructures.

For DoD, PIT/CS is employed in its broadest sense and represents the full range of control systems (SCADA, DCS, building, vehicle, transportation, etc.) located in DoD facilities. Moreover, CS is often installed piecemeal using commercial off-the-shelf (COTS) components, frequently by a variety of contractors using non-standard

equipment. Additionally, CS may be a loosely connected system of systems, typically consisting of a multi-facility front end, an installation-wide IP network, and multiple subsystems, all of which contributes to the broader environmental vulnerabilities to outside penetration. It is estimated there are tens of thousands of PIT/CS and their associated devices in use within DoD alone. In fact, DoD has yet to measure the scope and magnitude of the threats to which it may be exposed through its PIT environment.

A recent open-source analysis of fifteen PIT/CS attack vectors that have been successfully targeted against government/military/commercial industry environments since 2010 outlined specific instances where DOD missions could be impacted through PIT/CS with a high probability that several DOD PIT/CS may have already been compromised as they have in similar, civilian environments. As a case in point, in February 2015, Operation Cleaver identified Iranian hackers who attacked over 50 targets including DoD, defense contractors, and other critical infrastructure owners and stakeholders.

Fortunately, within the DoD there is a growing awareness of the PIT/CS vulnerability. In February 2016, the "8-star memo" was released by the commanders of NORTHCOM and PACOM, Admirals William E. Gortney and Harry Harris, respectively, to address PIT/CS in their areas of responsibility. The letter cites the "sevenfold increase in cyber incidents between 2010 and 2015 on critical infrastructure (e.g., Platform Information Technology (PIT) systems, Industrial Control Systems (ICS), and Supervisory Control and Data Acquisition (SCADA) systems) that control the flow of electricity, water, fuel, etc."[8]

The Cyber-Energy Nexus in an Operational Energy Context [9]

The focus now shifts to the energy sector and its unique set of cyber vulnerabilities. The most impactful and, arguably, the most vulnerable component of the shared civilian-military infrastructure is energy. Nowhere is this more prevalent than in the confluence of the virtual and physical domains evident in the cyber-energy space. As noted in PPD-21, energy and communications have converged to create an environment of exploitation of considerable magnitude. One notable recent example is the Black Energy attack of 23 December 2015 on a power plant in western Ukraine.[10] Perhaps more significantly, from a hybrid warfare and defense standpoint, this is manifest in vulnerabilities to the DoD's installation and operational energy environment. Though there are clear overlaps between installation and operational energy, this paper will focus on the operational aspects.

Why is Cyber-Energy Important in the Military Operational Field?

First, it is instructive to identify operational energy. Very simply, it is the energy needed to permit the warfighter to complete his/her mission.[11] Hence, the term operational energy as opposed to installation energy, which primarily addresses large, fixed and predominantly CONUS-based facilities. Moreover, operational energy is not a commodity but an enabler, with geostrategic and operational considerations. If we consider the operational energy component of the hybrid warfighter's tool kit, because of its enormous value in both the civilian and military operational spectrum, it provides a clear exploitation avenue by our potential adversaries. In the operational energy realm, this is most facility systems, to include water and waste treatment systems, micro grids, standby and prime generators, vehicle recharging stations, physical security systems and fueling systems.

This is coupled with the fact that there is greater, not less, demand for energy on the battlefield.

The new weapon systems are far thirstier than those being replaced, notable examples being the F-35 and many of the latest generation of ground combat vehicles. While ensuring these new platforms are faster, more mobile and better protected, the future demands for battlefield energy indicate this trend will not recede any time soon. This is not to mention the civilian supply-chain vulnerabilities, the means by which the majority of DoD liquid fuel is delivered on a global scale.

What we are learning at DoD is that the problem is larger than initially envisioned. For instance, there are unknown numbers of facilities with equally undefined numbers of physical assets being monitored. Moreover, there is no uniformity of products, processes, procedures or education and training required to monitor and maintain this vast technological environment. Thus, design and construction methods are changing to reflect new acquisition and cybersecurity requirements. This categorization also influences technology refresh cycles; while major equipment may last for 20-30 years, controllers and software/firmware are often obsolete in 1-5 years.

Some DoD Mitigation Efforts in the Cyber-Energy Realm

One program within the DoD which addresses the full scope of threats across the enterprise is the Joint Mission Assurance Assessments (JMAA). These assessments are performed by combined teams which collect, analyze, and store assessment results in unified information management tools. Such consolidated efforts increase information sharing and provide comprehensive understanding of mission risk. The JMAAs also provide standardized assessment benchmarks, which communicate known risks to decision makers and program managers. And while the JMAAs consider an all-hazards approach to the DoD enterprise, cyber is a large and growing component.

Moreover, specific mitigation efforts in the DoD installation and operational energy sectors are underway, measures which could be used as templates for broader and more advanced analysis. The Office of the Deputy Assistant Secretary of Defense for Operational Energy [12] is sponsoring a study performed by Johns Hopkins University's Applied Physics Lab on the DoD PIT/CS environment writ large.[13] A case study featured in this analysis comprises a sizeable energy infrastructure component. Numerous DoD facilities were analyzed, all in the continental United States.

This effort is also intended to help address these challenges and provide senior leaders with an accurate account of the exploitability of these systems and to enhance and enable appropriate resource decisions. The research follows a repeatable methodology to analyze key infrastructure at a technical level and to identify attack or potential attacks against critical PIT/CS infrastructure. Additionally, the methodology identifies network connectivity, especially external connections and vulnerabilities in the system that could be exploited with sufficient access. Best practices, security architectures, security controls and/or compensating controls that increase resilience to known attack tools and techniques will also be included in this analysis.

Ultimately, this analysis will help provide:

1. Solutions for both operational energy and installation energy missions
2. Analysis to guide future research and development
3. Collaboration and professionalism of DoD PIT/CS stakeholders/workforce
4. Solution that are relevant, cost effective and usable across military departments
5. Draft mitigation strategy to close the cyber gaps.

More specifically, Johns Hopkins is addressing three primary areas in the PIT/CS environment: 1) Threats; 2) Gaps/Vulnerabilities, and 3) Skills sets. Task 1 is dedicated to the physical environments of the DoD sites analyzed. Tasks 2 considers Government, industry and academia's analytic capabilities to detect, respond and recover from cyber-attacks, while Task 3 analyzes the types of skills which will be most valuable in the future. Johns Hopkins has done a superb job in its analysis and we look forward to their final report.

Interagency and International Cooperation

A key to addressing the cyber threat in the PIT/CS realm is a coordinated and comprehensive countermeasures effort. Indeed, as hybrid warfare ranges across the military and civilian domains, so does the broader U.S. Federal and civilian response, all the more important as operational energy relies on the civilian infrastructure. The North American Electric Reliability Corporation (NERC), a civilian non-profit organ-

ization which establishes national reliability standards, issued the NERC-CIP (Critical Infrastructure Protection) standards.[14] Moreover, the National Institute of Standards and Technology (NIST) has created the cyber security framework which is adhered to by both civilian and military Federal agencies.[15]

Intra-agency cooperation also exists, notably between DoD and the Departments of Energy (DoE) and Homeland Security (DHS), though clearly such links also exist throughout the U.S. Government.[16] The DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) is a leading proponent of cyber risk reduction strategies.[17] The DOE's national lab system is a tremendous asset which conducts a variety of advanced cyber defense research, notably Pacific Northwest National Labs, as well as Sandia and Idaho National Labs. Furthermore, the private sector is heavily engaged, such as Cisco, IPERC, Schneider Electric and Honeywell.

To flesh out the Government, industry and academia triad, U.S. universities provide valuable research and development contribution. In addition to Johns Hopkins University, there is the Naval Postgraduate School, Massachusetts Institute of Technology, and Virginia Tech, which have contributed to our efforts. Again, this list of Government, industry and academia participation in the PIT/CS environment is not intended to be inclusive, but merely to highlight some of the excellent support DoD has received in this area.

The global nature of the PIT/CS environment and the equally dispersed locations of the threat necessitates an international response, such as the venue where we are gathered today. This includes intelligence sharing and cooperative efforts in cyber defense education and training. Such international cooperation includes friends and allies

around the world, such as NATO's Cooperative Cyber Defense Center of Excellence [18] in Tallinn, Estonia, as well as the German cyber defense institute, CODE, headquartered at the Bundeswehr University in Munich.[19] One annual venue of note, the European Conference on Cyber Warfare and Security has been in effect for 16 years now, where participants meet to speak on a range of cyber-related defense issues.[20] Finally, I would be remiss if I failed to mention the work of the Armed Forces Communications and Electronics Association, of which the Sofia Chapter is co-organizer of this event. It is precisely through this ability to bridge government, industry and academia which permits a comprehensive and coordinated response to the threat.

Conclusion

This paper is in itself a sort of hybrid compilation and exemplifies the fluid nature of the threats we are facing across multiple government functional areas and economic sectors. Hybrid warfare, whether instigated by a state or non-state actor, has the capacity to cause loss of life or property damage, and for this reason must be taken seriously with efforts undertaken to mitigate risk or lessen its impact. Narrowly focused on the Operational Energy perspective, attacks to the DoD energy infrastructure have the potential to impact mission success and unit readiness. Moreover, it is imperative we understand that the problem will not recede any time soon, particularly as we attempt to achieve net-based efficiencies. Also, the pervasive condition of the cyber environment and the truly global nature of the problem necessitates an inter- and intra-governmental cooperative effort.

As the confluence of cyber and energy continues, and the demand of the warfighter on energy, this threat will not subside any time soon. Therefore, hybrid warfare, whatever form it takes in the future, will continue to be with us, presenting both challenges and opportunities for defense professionals in the form of infrastructure resilience, brought about by redundant systems or hardening. By necessity, and in the interest of space and time, much has been omitted from this paper. However, this paper was designed to foster discussion and international cooperation in the broader hybrid warfare realm, one of its newest and most insidious threats against critical infrastructure, both within and without the defense industry. I welcome the opportunity to engage with my colleagues in this forum to exchange information and best practices in the months and years going forward.

Disclaimer

Views presented are those of the author and do not reflect official DoD policy

Notes

[1] Presidential Policy Directive 21 (PPD-21) identifies both energy and communications as "…uniquely critical due to the enabling functions they provide across all critical infrastructure sectors." See The White House, "Presidential Policy Directive – Critical Infrastructure Security and Resilience," No. PPD-21, February 12, 2013, www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[2] United States Government Accountability Office, "GAO-10-1036R Hybrid Warfare," Briefing to the Subcommittee on Terrorism, Unconventional Threats and Capabilities, Washington, DC, September 10, 2010, http://www.gao.gov/assets/100/97053.pdf.

[3] Frank Hoffman, "On Not-So-New Warfare: Political Warfare Vs Hybrid Threats," *War on the Rocks*, July 28, 2014, http://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/.

[4] Julian Lindley-French, "NATO and New Ways of Warfare: Defeating Hybrid Threats," *NDC Conference Report*, no. 03/15 (Rome: Research Division, NATO Defense College, May 2015), http://www.ndc.nato.int/news/current_news.php?icode=814.

[5] For a description of the Service Components' efforts in this space, see U.S. Cyber Command Combined Action Group, "Beyond the Build: How the Component Commands Support the U.S. Cyber Command Vision," *Joint Force Quarterly* 80 (1st Quarter 2016): 86-93.

[6] Department of Defense Instruction (DoDI), "Cybersecurity," 8500.01, 14 March 2014, p. 39, http://dtic.mil/whs/directives/corres/pdf/850001_2014.pdf.

[7] This is also called Industrial Control Systems (ICS).

[8] "Eight Star Memo – Admirals William Gortney and Harry Harris to Ash Carter," February 11, 2016.

[9] See Nussbaum, Daniel A., Stefan W. Pickl, Arnold C. Dupuy, and Marian S. Nistor, "The Nexus Between Cyber Security and Energy Security," in *Proceedings of the 15th European Conference on Cyber Warfare and Security (ECCWS2016)*, ed. Robert Koch and Gabi Rodosek, Munich, Germany, July 2016, pp. 228-236.

[10] ICS – CERT, "Cyber-Attack Against Ukrainian Critical Infrastructure," IR-ALERT-H-16-056-01, Department of Homeland Security, February 25, 2016, https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

[11] US Department of Defense, "2016 Operational Energy Strategy," Office of the Assistant Secretary of Defense for Operational Energy, February 2016, http://www.acq.osd.mil/eie/Downloads/OE/2016%20DoD%20Operational%20Energy%20Strategy%20WEBc.pdf.

[12] Office of the Assistant Secretary of Defense for Energy, Installations, and Environment, "Operational Energy," http://www.acq.osd.mil/eie/OE/OE_index.html.

[13] Johns Hopkins Applied Physics Laboratory, http://www.jhuapl.edu/.

[14] North American Electric Reliability Corporation, "Critical Infrastructure Standards," http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

[15] NIST Cybersecurity Framework, http://www.nist.gov/cyberframework/index.cfm.

[16] There should also be acknowledgement of the cooperation of the Department of Justice (FBI) and the Director of National Intelligence.

[17] https://ics-cert.us-cert.gov/.

[18] https://ccdcoe.org/about-us.html.

[19] https://www.code.unibw-muenchen.de/aktuelles.

[20] http://www.academic-conferences.org/conferences/eccws/eccws-future-and-past.

About the Author

Arnold C. Dupuy holds a Ph.D. degree in Planning, Governance and Globalization with a concentration in International Energy Security from the Virginia Polytechnic Institute and State University, Alexandria, VA (2016). With twenty-five years of military experience (active and reserve status), he is currently Assistant adjunct professor of political science at Virginia Tech, with a concentration in international politics and energy geo-politics and Booz Allen Hamilton Associate.