Cybersecurity in the Energy Sector An Analysis

Serhat S. Çubukçuoğlu
serhat.cubukcuoglu@alumni.tufts.edu

1. Introduction

In the New World Order of the 21st century, the information age has revolutionized our lives, shrunk distances, and made societies more interdependent. Cyberspace and its underlying systems emerged as domains of profound influence on defense doctrines with the advent of communications technology, proliferation of the Internet and networked devices so-called the "IoT" (The Internet of Things). Virtual warfare, waged via computers and the Internet, became an essential aspect of military conflicts between adversaries, as the operation and management of warfare in the future has begun to change.[1] To policymakers, possession of fastest computers is as crucial in the 21st century as possession of longest-range aircraft was in 20th century. Just as airpower had transformed battle scenes back then, the military utility of cyberspace has risen with diffusion of asymmetric warfare, which, in essence, is the goal of a war: One side will inevitably want to dominate over the other and make the balance asymmetric.[2] As a form of smart power, cyberpower emboldens low-profile actors, decreases threshold of turning points in crises, and multiplies kinetic power's impact. Since the very orality of the Internet has a way of turning territorial battles into battles of ideas,[3] transformation of modern battles utilises de-territorialised cyber attacks as means of persuasion and winning hearts and minds on a mass scale.[4] In the information age, what's important is not just "whose army wins in battle, but whose story wins over people".[5]

News headlines highlight incidents about private firms, government institutions, agencies, and critical infrastructure as frequent targets of increasingly sophisticated cyber weapons and techniques utilized by criminal organizations, state-sponsored terrorist, belligerent non-state actors, as well as national armed forces. Depending on an assailant's motivation and desired impact on the target, malicious activities on cyberspace aim to subdue victims through data loss, financial gain, espionage, damage to commercial, physical assets, and disruption of supply chain, transportation, communication, and geo-location systems. Political actors are targeted during election campaigns through perceptual manipulation of public opinion over ads, spam, spoofing, and phishing attacks through cyberspace. The real power of cyber is in fact its potential cascading effects on other domains. Since it enables a strike directly and immediately aimed at the seat of the opposing will and policy, it diminishes the decisiveness of major wars.[6] Missile tests, nuclear detonations, and advanced Artificial Intelligence (AI) platforms precipitate cyber responses that may spiral into a full-scale conflict in high-risk profile regions.

Energy sector, inevitably, is among the most frequently targeted critical service fields in the world. Vengeful acts of malware attacks on the Persian Gulf's energy sector,

sabotage attempts on chemical plants in Saudi Arabia, blackouts in Turkey's electricity grid, and hacks against the U.S. infrastructure are on everyday news headlines. Increased threat level on energy sector has ramifications on water, sewage, health, and communication services,[7] putting more pressure on governments and companies to scrutinize security of their IT network hardware, keep software up-to-date, encrypt information and train their staff on best practices on cyber space. Moreover, the advent of blockchain technology incentivized peer-to-market and peer-to-peer transfer of energy assets that requires secure, scalable, and efficient methods to ensure operability and adoptability. Distributed ledgers are vulnerable to cyber attacks if proper security measures and practices are not observed, the key being people skills and awareness to keep risks under control. Recently, the future of the JCPOA to curb Iranian nuclear ambitions fell into uncertainty due to the U.S. threat to pull out, leaving the Middle East once again as a playground for escalatory tit-for-tat moves. It is fresh in memories how nuclear facilities became a target of malware attacks and yet the extent of catastrophic consequences that it could have unleashed is still not fully conceived. This opaque, behind-the-scenes type asymmetric warfare is the most dangerous of all kinds since previous notions of deterrence do not necessarily provide adequate safeguards to prevent escalation.

2. Cybersecurity and Hybrid Warfare

For 400 years, those who possessed the greatest power in the global commons, especially at sea, have been able to exert dominion over those who do not. Cyberspace, on the other hand, appears to empower challengers to resist against hegemony.[8] Insurgents, armed groups, terrorists, political fractions of all sorts can exploit vulnerabilities of nations states by using "hacktivist" techniques to further their cause and undermine the global order.[9] Above all, cyberspace has the potential to promote social and political change, as seen by the transformative effect of social media on politics in the Middle East and North Africa, and furthermore to "alter the configuration of the global commons".[10] The Internet is the new battlefield, social networks are the weapons, and states, non-state actors, and citizens are its combatants.[11]

Cyber warfare may not resemble conventional war but damages can be as crippling. Perhaps most importantly, since cyberspace is ubiquitous, it affects all aspects of life, rendering it highly unlikely that future conflicts will unfold in exclusively one domain. Due to its low buy-in cost and as a multiplier of physical force, cyber warfare can generate "catastrophic cascading effects through asymmetric operations".[12] A cyber attack can target a nation's "nervous system"[13] behind the protective barriers of physical battlefronts, and as such, its principal goal is to persuade and subdue the enemy through strategic communication without fighting, thus framing a conflict in an ideologically advantageous way that enables direct influence over societies.[14] Iran, for instance, uses a mix of threats and forces to employ intimidation as a form of asymmetric warfare.[15] A cyber espionage group linked to the Iranian government recently attacked energy, military, and aerospace targets in Saudi Arabia, South Korea, and the U.S.[16] A war does not necessarily involve conflict, and, as Sun Tzu says in his famous work "The Art of War", Iran's aim is to win the war without fighting the war.[17]

In hybrid wars, states and non-state actors blend high-tech capabilities, like anti-satellite weapons, cruise missiles, and Intercontinental Ballistic Missiles (ICBMs) with terrorism and cyber warfare.[18] Russia allegedly uses disinformation and propaganda in synch with cyber attacks and military show-down against Baltic states, Finland, and Norway.[19] This emerging form of warfare includes the entire society and necessitates a comprehensive escalation strategy to integrate vulnerabilities into a robust security infrastructure for effective crisis management. This is a complex world of confrontations and conflicts rather than one of war and peace.[20] In non-traditional, irregular warfare, "netwar" as a form of low-intensity cyber warfare suits the definition of cross-domain warfare in the 21st century. Empowered non-state or sub-state actors utilize cyberspace to organize their constituents and challenge central authorities of nations. ISIS, for example, uses cyberspace as a propaganda platform to shape the "information environment" of conflict[21] and gain public support, enabling it to wage a leaderless warfare. This distinct strategic character and concept of operations[22] necessitates an inter-agency connected specialist counter-terrorism task force suited for cyber defense with a flat, de-centralized structure to increase crisis response agility.

Regrettably, prospects for defense against cyber attacks are not good. Firewalls can be breached, people can be exploited, and systems can fail to detect intruders. Open societies such as the U.S. have promiscuously networked their systems in ways that make it very difficult to disconnect from the Internet.[23] Despite earlier warnings from Israel to its U.S. counterparts,[24] Russian state-sponsored hackers were able to conduct cyber espionage on the NSA material from a contractor's laptop through Kaspersky Lab's ant-virus software.[25] Cyber arms are easily found on the dark web or off-the-shelf. If insurgents can use the tools of globalization against itself and can cross all of the organizational boundaries, so must the defense systems: There is need to have a holistic approach to cyber defense.[26] The goal is to pro-actively build capabilities to be superior at each level of escalation in crises across domains and boundaries. With this goal, the U.S. Department of Homeland Security, for instance, aligns agencies for new types of crises including cyber attacks to minimize the impact of "unknown unknowns" while fostering organizational development of national crisis management. Following the attack on NHS in 2017, the UK has increased funding for GCHQ to make it a "cyber-organization" as much as an intelligence and counter-terrorism one.[27] Similarly, the first EU ministerial-level cyber exercise conducted in Estonia was based on a fictional scenario that "moved from a minor cyber incident up to a real blockade of communications systems that stopped a naval operation on the Mediterranean."[28]

3. Crisis Management in 21st Century Warfare

Crisis management in statecraft is the art of using time and space to advance one's gains,[29] especially by turning dangers into opportunities. It takes place at a crucial time during when there is high probability of hostilities due to perceived threat to vital interests. How a crisis may unfold, escalate, and whether it can be prevented are of prominent concern for the pre-crisis phase. Deterrence is of crucial importance to prevent escalation of crisis and cybersecurity has a large role in crisis management. In this re-

gard, escalation dominance is an indispensable and desirable aspect of successful crisis management, which can take kinetic form, with armed forces, or non-kinetic form, with cyber weapons that serve as a platform of attacks on information systems. In pre-crisis phase, cyber escalation as a basis for cyber deterrence becomes much more salient.[30] As sophisticated cyber threat actors are ever growing, North Korea, for instance, has acquired capabilities to attack the South prior to testing its new arsenal of nuclear weapons and missiles. Pyongyang has the cyber power to incur as much damage as possible against military, infrastructure, and industry complexes in a conflict situation, and frequently does cyber reconnaissance to prepare for war with the South. If it breaks out, during war time, North Korea may launch cyber attacks,[31] and as a response the allied cyber command can provide means to penetrate, disrupt, and corrupt North Korea's networks.[32] Cyber capabilities can give the U.S. Navy Seals the advantage on the ground, ensure that satellites have the most accurate positioning for a laser-guided missile attack, and respond to domestic civil unrest in the South.

Essentially, escalation and de-escalation of 21st century crisis can take place across all domains of warfare: Land, Sea, Air, Space and Cyber. In cross-domain warfare, the platform in which the attack is launched and where its effects are felt may be different. Firstly, anonymity and intangibility of cyber attackers are undermining factors against efforts to prevent crisis from turning into war. At the onset of a crisis, with the identity of cyber attackers possibly unknown, making retaliation difficult, elusive decision-making may lead to escalation of hostilities.[33] An effective means to deter a major war may prove ineffective.[34] Secondly, cross-domain escalation resembles horizontal escalation in that one side has a perceived advantage over the adversary, although, unlike horizontal escalation, crossing a geographic threshold may not necessarily be a pre-requisite to be considered as an escalatory move. During Korean Missile Crisis, the U.S. had a military advantage around the Western Pacific whereas North Korea had an advantage around the peninsula: Taking positions and showing of capabilities was a potential horizontal escalation from Korea to the Pacific, but it does not need to involve use of physical force. Cross-domain warfare is characterized by effects-based operations: if intended consequences of a particular type of action within a domain unfold in a different domain, it makes possible to realize synergies between domains. Kinetic attacks against cyber facilities or cyber attacks against kinetic weapon systems highlight the relationship between kinetic and non-kinetic forces with regard to crisis escalation.

As for the energy sector, on one hand, nuclear plants in the U.S. operate on high assurance environments, monitored, maintained and isolated from the Internet against cyber threats. North Korea or Iran may not be able to attack a U.S. aircraft carrier but may do so to those facilities that enable these systems to destroy intended targets,[35] such as the GPS satellite network. Indeed, it is possible that cyber attackers might have engineered the collision between the U.S. Navy ship USS Fitzgerald and a container ship off the coast of Japan via an intrusion on the networked control system and disruption to GPS navigation.[36] On the other hand, Israel may not be able to preemptively attach an Iranian nuclear enrichment facility with kinetic force at peace time but may exploit security loopholes to penetrate cyber defenses and inflict irreparable damage upon critical infrastructure. The weakest link in such a case often proves to be human-error rather than processes or the technology. Of special worth to note is that Dubai utilities company

DEWA has launched the world's first autonomous, renewable energy utility offering Artificial Intelligence (AI)-powered digital services, as an exemplary case of a disruptive business model that requires greater attention to emerging technologies, vulnerabilities, and opportunities for cybersecurity. The city is fast evolving, embracing futuristic technologies, and hosted the world's first AI show in April 2018 amid smart city ambitions.[37]

Crisis readiness in cyber warfare requires acute awareness of potential vulnerabilities, ability to pick, analyze, and act upon the right information and inter-agency coordination. Tackling with cyber aggressors should not be left only to capabilities of IT professionals, who are more common, but rather involve people with diverse skills and backgrounds to make sense of vastly increasing amounts of big data through the proliferation of social networks.[38] Using simulations, crisis gaming, and imagination[39] can help connect the dots, increase agility, and facilitate cyber threat assessment. During the 9/11 attacks in New York, there was a need for the Federal Aviation Administration (FAA) to ground all flights within the first few hours, which could be facilitated by a cyber swat team. Post 9/11, the U.S. and its allies deployed a variety of military capabilities with the intent to destroy terrorists and those who harbor them. As an escalatory option, it included the policy of pre-emption based on actionable intelligence. In cyber domain, this meant the opening of a door to a new era of escalation, as exemplified in the use of Stuxnet computer virus by the U.S. and Israel's covert action forces against Iran's nuclear program. In a similar fashion, China has often used cyber weapons against the U.S. government computer systems and contractors with the motive to map "military capabilities that could be exploited during a crisis".[40] The goal being to take a picture of the U.S. defense networks, logistics, and related military capabilities that could be targeted during a crisis, cyber weapons have become integral to Chinese military strategy and it is estimated that 90% of cyber-espionage in the U.S. originates from China.[41]

4. Conclusion

Cybersecurity is a vital component of combined operations in modern warfare. It can be used by states, armed groups, insurgents, and terrorists as a powerful tool to gain asymmetric advantage, impose demands, and subdue opponents. Nevertheless, notwithstanding cutting-edge capabilities that cyber space provides, like any other advanced technology, it cannot be a pure play option for warfare. It is highly unlikely that cyber attackers from outside can breach a nuclear plant to trigger a disaster, but human factor should not be discounted as a major cause of cyber incidents. Blockchain-based de-centralized systems create cyber vulnerabilities if proper security measures are not incorporated into technology architecture from the outset. As a force multiplier for kinetic power, cyber can be put to divide, dishearten, and disrupt an adversary's will to fight, gather intelligence and trigger a crisis by subverting network defenses. Cyber attacks may be perceived as escalatory signals in a crisis setting and precipitate kinetic responses, or vice versa, laying clear the increasingly cross-domain character of military hostilities. Serious impact on a state's critical infrastructure, economy, and reputation, even if non-lethal, may grant the right to invoke the U.N. Article 51 for self-defense. In the 21st century's hybrid warfare, cyber domain will be a central part of conflicts and complement other domains for both states and non-state actors as armed groups use it to their advantage to dominate their adversaries. It requires more than just military hardware, but also training,

public awareness, and cross-agency cooperation to survive in this new normal.

Endnotes

1 Dr. Jamal Sanad Al-Suwaidi, "The Future of Warfare in the 21st Century", ECSSR, April 9-10, 2013.

2 Dr. Austin Long, "The Future of Warfare in the 21st Century: Asymmetrical Warfare and International Terrorism", ECSSR, April 9, 2013.

3 Robert Kaplan, "The Revenge of Geography," Random House Trade Paperbacks, Reprint edition, 2013, p. 128.

4 David J. Betz and Tim Stevens, Cyberspace and the State: Toward a Strategy for Cyber-Power (New York: Routledge, 2011), Ch. 4.

5 David J. Betz and Tim Stevens, Cyberspace and the State: Toward a Strategy for Cyber-Power (New York: Routledge, 2011), Ch. 3.

6 David J. Betz and Tim Stevens, Cyberspace and the State: Toward a Strategy for Cyber-Power (New York: Routledge, 2011), Ch. 3.

7 The Financial Times, "Energy sector on alert for cyber attacks on UK power network," Sylvia Pfeifer, Nic Fildes, Aliya Ram, April 18, 2018 (accessed April 19, 2018); available from https://www.ft.com/content/d2b2aaec-4252-11e8-93cf-67ac3a6482fd.

8 David J. Betz and Tim Stevens, Cyberspace and the State: Toward a Strategy for Cyber-Power (New York: Routledge, 2011), Ch. 4.

9 Ibid.

10 Ibid.

11 John Bassett OBE, "The Future of Warfare in the 21st Century: Cyber Security", ECSSR, April 9, 2013.

12 David J. Betz and Tim Stevens, Cyberspace and the State: Toward a Strategy for Cyber-Power (New York: Routledge, 2011), Ch. 3.

13 Ibid.

14 Ibid.

15 Dr. Anthony Cordesman, "Iran and the Threat to "Close" the Gulf", CSIS, Burke Chair in Strategy, 2011, p.32.

16 OSAC, "Iranian Hackers Target Aerospace, Energy Companies," Weekly Cyber Security Awareness (accessed October 5, 2017); available from http://www.securityweek.com/iranian-hackers-target-aerospace-energy-companies.

17 Dr. Anthony Cordesman, "The Future of Warfare in the 21st Century: Conflict and Order in the Middle East", ECSSR, April 10, 2013.

18 David J. Betz and Tim Stevens, Cyberspace and the State: Toward a Strategy for Cyber-Power (New York: Routledge, 2011), Ch. 3.

19 Foreign Policy, "Russia's Neighbors Respond to Putin's 'Hybrid War'," Reid Standish, October 12, 2017 (accessed October 15, 2017); available from http://foreignpolicy.com/2017/10/12/russias-neighbors-respond-to-putins-hybrid-warlatvia-estonia-lithuania-finland.

20 Ibid.

21 David J. Betz and Tim Stevens, Cyberspace and the State: Toward a Strategy for Cyber-Power (New York: Routledge, 2011), Ch. 4.

22 David J. Betz and Tim Stevens, Cyberspace and the State: Toward a Strategy for Cyber-Power (New York: Routledge, 2011), Ch. 3.

23 David J. Betz and Tim Stevens, Cyberspace and the State: Toward a Strategy for Cyber-Power (New York: Routledge, 2011), Ch. 3.

24 The Washington Post, "Israel Hacked Kaspersky, then Tipped the NSA that its tools had been breached," Ellen Nakashima, October 10, 2017 (accessed October 15, 2017); available from https://www.washingtonpost.com/world/national-security/israel-hacked-kaspersky-then-tipped-the-nsa-that-its-tools-had-been-breached/2017/10/10/d48ce774-aa95-11e7-850e-2bdd1236be5d_story.html.

25 The Wall Street Journal, "Russian Hackers Stole NSA Data on U.S. Cyber Defense," Gordon Lubold, Share Harris, October 5, 2017 (accessed October 15, 2017); available from https://www.wsj.com/articles/russian-hackers-stole-nsa-data-on-u-s-cyber-defense-1507222108.

26 John Bassett OBE, "The Future of Warfare in the 21st Century: Cyber Security", ECSSR, April 9, 2013.

27 OSAC, "Cyber-security Threat to UK 'as serious as terrorism' - GCHQ," Daily Intelligence Digest, BBC, October 10, 2017 (accessed October 15, 2017); available from http://www.bbc.co.uk/news/uk-41547478.

28 OSAC, "Cyber Defense Is Very Much About Political Decisions," Weekly Cyber Security Awareness (accessed October 5, 2017); available from http://www.govexec.com/defense/2017/09/cyber-defense-very-much-about-political-decisions/141234/.

29 Prof. Robert Pfaltzgraff, "Security Studies and Crisis Management", The Fletcher School of Law and Diplomacy, Tufts University, 2014.

30 Ibid.

31 Sorana Parvulescu, Partner, "Korean Peninsula: Threat Monitoring and Advisory", Control Risks, Dubai, October 10, 2017.

32 David J. Betz and Tim Stevens, Cyberspace and the State: Toward a Strategy for Cyber-Power (New York: Routledge, 2011), Ch. 3.

33 Ibid.

34 Ibid.

35 Prof. Robert Pfaltzgraff, "Security Studies and Crisis Management", The Fletcher School of Law and Diplomacy, Tufts University, 2014.

36 Hellenic Shipping News, "Not Just Somali Pirates, Cyber Attacks Too Hit Ships," December 11, 2017 (accessed December 17, 2017); available from http://www.hellenicshippingnews.com/not-just-somali-pirates-cyber-attacks-too-hit-ships/.

37 Arabian Business, "Dubai to host first World AI Show amid smart city ambitions", March 23, 2018 (accessed March 25, 2018); available from http://www.arabianbusiness.com/technology/392636-dubai-to-host-first-world-ai-show-amid-smart-city-ambitions.

38 Prof. W. K. Wark, "Annual Conference: War in 21st Century, Information and Intelligence in the 21st Century", ECSSR, April 9, 2013.

39 The 9/11 Commission Report, Authorized Edition, 1st Edition, W.W. Norton & Company, p. 347, 357.

40 The New York Times, "US accuses China's Military in Cyberattacks," May 7, 2013, (accessed October 12, 2017); available from http://www.nytimes.com/2013/05/07/world/asia/us-accuses-chinas-military-in-cyberattacks.html?_r=0.

41 Ibid.