KGRI Working Papers
No. 1

Society-Centric Cyber Conflict
Understanding its dynamics and potential in East-Asia

Version 1.0

August 2021

Tobias BURGERS and David J. FARBER
Cyber Civilization Research Center (CCRC)

Keio University Global Research Institute

Research Institute, Keio University and David J. FARBER, Co-director, Cyber Civilization Research Center, Keio University Global Research Institute & Distinguished Professor, Keio University

Society-centric cyber conflict.[1][2]

Understanding its dynamics and potential in East-Asia.

Tobias BURGERS and David J. FARBER
Keio University, Cyber Civilization Research Center (CCRC)

Executive Summary: This paper discusses the recent and worrisome increase in cyber-attacks that target critical infrastructure. We argue it is essential to better understand these attacks and their impact. By providing an analytical framework, we measure the impact of such attacks and argue that attacks with societal impacts trigger a new form of cyber conflict which we define as society-centric cyber conflict (S3C). We argue that in S3C, we must better understand the societal dimension of cyber conflict: It is necessary to understand a) the societal impact of cyber-attacks and b) societal reactions to the impact of such attacks, and c) how societal reactions could influence the dynamics of cyber conflict. We argue that these variables are specifically crucial in understanding the escalation dynamics in cyber conflict.

Highlighting the lack of data on societal impact and reactions, we provide a methodological approach to gather much-needed data and make a case for further research on S3C – in specific in the Asian-Pacific region where we believe the significant potential for S3C exist with implications for regional cybersecurity dynamics and (broader) security relations.

[1] Tobias Burgers is a project assistant professor at the Cyber Civilization Research Center, Keio University. David J. Farber is the co-director of the Cyber Civilization Research Center and a distinguished professor at Keio University.

[2] The authors wish to thank Jiro Kokuryo for his comments and review.

1. Societal-centric cyber-attacks and the rise of society-centric conflict

The discovery of the Stuxnet operation set of a digital firestorm: While the sophistication of the attack led to much discussion, so did the purpose of the operation: The physical degradation of Iran's nuclear centrifuges, used for Iran's military nuclear development program. The Stuxnet operation was the first known cyber operation intended to cause disruption and damage in the physical domain. Prior known cyber incidents could be categorized in three other types of cyber operations, namely, disruption, and short term and long-term espionage, with targets in the digital domain and without the explicit aim to degrade or destroy physical targets (Valeriano and Maness, 2018). A decade later, we can conclude that the Stuxnet was the forebear of a current wave of much more offensive cyber assaults which aim to cause physical disruptions or destructions. Stuxnet-like cyber operations are becoming what Glosserman (2020) refers to as the "new normal." Glosserman (2020) and others list an array of examples of this new normal: cyber-attacks on Israeli water facilities and Iranian harbor infrastructures, the 2018 Saudi petrochemical plant attack, the Shamoon attack on the Saudi oil giant Aramco, the Iranian cyberattacks of US dams, the Russian attacks on the Ukrainian power grid and most recently the Chinese attack on the Indian power grid (Healey & Jervis, 2020; Glosserman, 2020; Perlroth & Krauss, 2018; Recorded Future, 2020; Schneider, 2020). The rise of such attacks has given way to debates in which cyber doomsday scenarios are a regular presence. According to some experts, we are facing a "Cyber Pearl Harbor," a "Cyber 9/11", a "Cyber Black Swan" or a Cyber Armageddon" (Bumiller & Shanker 2012; Goldman & Warner, 2017; Herbolzheimer, 2016; Lawson & Middleton, 2019). Often invoked examples of such doomsday attack scenarios are the destruction of power grids, a potential meltdown of nuclear powerplants, interruption and destruction of transportation systems and water distribution systems, the destruction of financial data, crashing the financial system, disruption and destruction of medical services, and hacking of air traffic control centers (Glosserman, 2020; Greenberg, 2019a; 2019b).

Given the potential societal devastation in these scenarios, not surprisingly, these attacks have triggered a debate about the direction cyber conflict is taking (Greenberg, 2019a). Are we on the verge of such cyber doomsday scenarios turning into reality? What are the consequences if actors engage further in cyber-attack campaigns that target critical infrastructure? If such attacks cause societal impacts how would nations react to such attacks? Would they seek retaliation? If so, by what means? Could such cyber-attacks set of action-reaction cycle that spirals into armed conflict (Libicki, 2020)? While it is subject to debate if such doomsday scenarios will occur, we argue that it is nevertheless it is reasonable to believe that cyber-attacks against civilian targets, particularly infrastructure, are likely to increase; An environment with ample critical infrastructure targets exists while sufficient cybersecurity defenses, measures and attention by the respective actors in control of such infrastructure are lacking. This is so in particular vis-à-vis critical military targets which are a lot better resourced, defended and as such harder to successfully target and penetrate. Then there is the perception that civilian targets would be less dangerous to target than military targets. Finally, as the examples above illustrates, there is a decreased hesitancy to attack such targets. The sum of this contributes to a scenario in which what we refer to as societal-centric cyber attacks are predicted to increase in frequency (Rovner, 2021).

The rise of societal-level cyber-attacks has the potential to change and reshape the dynamics of cyber conflict. To date, much of the conflict in the cyber domain has had a limited societal impact, with the public only limitedly exposed to the effects of cyber attacks. However, the foreseen increase of societal-level cyber attacks ensures that populations will increasingly notice the effects and impact of cyber attacks. To paraphrase Zac Rogers (2019), "populations, not soldiers, are now on the front lines." If populations are becoming part of cyber conflict, the frontline even, we argue it is critical to understand what Levite and Shimshoni (2018) refer to as the social dimension of conflict. In their essay, the authors introduce the concept of society-centric warfare as a framework to understand how societies deal with and react to threats and attacks with societal impacts and how its perceptions and reactions influence conflict dynamics. Building further on their research, we seek to extent their framework to the cyber domain to understand how societies could react to cyber-attacks with societal impact(s). Thus, we argue that we need to develop an understanding of what we refer to as society-centric cyber conflict (S3C).[3] We view society centric cyber conflict as a type of cyber conflict in which actors attack targets that are critical for the functioning of societies, with successful attacks causing societal impact(s). While this definition gives an initial starting point for understanding S3C, it needs further clarification. In particular what are considered targets that are critical for the functioning of societies, and secondly how we understand, define and measure societal impact. We consider critical targets, targets that are considered part of a nation's critical infrastructure. Analyzing the US', EU' and Japan's definitions of critical infrastructure we define six sectors as critical for the functioning of societies (CEU, 2008; CISA 2020; CSH, 2017; Jhangiani and Kennis 2021)[4]:

- Communication sector (e.g. telecommunication services and -infrastructure)
- Financial sector (e.g. banks, banking)
- Healthcare and medical sector (e.g. hospitals)
- Governmental sector (e.g. police and other security organizations, local, regional and national public governments, emergency service)
- Transportation sector (e.g. railways, bridges, highways, harbors, airports, train stations, public transport networks)
- Utilities sector (e.g. water works, electricity provider, sewer systems, power grid)

Successful attacks against targets in these sectors have the potential to threaten the functioning of societies. Yet if such attacks will threaten such is equally a question of target attacked, as a question of the impact of such an attack: An attack against targets in these sectors would not necessarily have a societal impact. An attack against public infrastructure, such as bridge in a remote area with its functioning disrupted or destroyed, would have impact that would not necessarily be noticeable throughout society. Thus, we need define further how we measure societal impact and build a framework that allows us to measure

[3] Levite and Shimshoni (2018) use the term warfare in their analysis. The notion of war(fare) in the cyber domain remains contested and as such instead we will use the term conflict. For further information and discussion on the concept of war in the cyber domain and cyber warfare, see Rid, T. (2017). *Cyber war will not take place*. Oxford University Press.

[4] Jhangiani and Kennis (2021) note the problems and ambiguity of (exactly) defining what are critical infrastructure targets. Therefore, rather than engaging in a discussion what are exactly such targets, we chose to list sectors of critical infrastructure, which are more commonly accepted and defined.

societal impact across various nations and cases. To define and measure this impact we build further on the analytical framework of Healey et al (2020). In their study on disruptive cyber operations the authors argue impact is defined by two variables. First, the effect of such operations. Second, the duration, with duration defined by the authors as "an estimate of how long it takes the adversary to return to initial operating capability (able to conduct some limited operations) and return to full operating capability (approaching the full range of the adversary's previous activity) (Healey et.al. 2020, p.254). [5] Reinterpreting Healey et.al.'s (2020) framework, we use the same variables and develop this into the following framework to measure societal level impact. The first variable is the potential disruptive and destructive effect of cyber-attacks against targets which are part of critical infrastructure. We measure the disruptive or destructive effect according to the scale as used by Healey et.al (2020):

- Minor effect: Slight impact;
- Significant effect: Intermediate impact;
- Decisive effect: Substantive impact"

We measure duration in a simplified four-point scale as used by Healey et.al. (2020):

- Days to weeks;
- Weeks to months;
- Months to years;
- Never.

From this we define societal impact as an impact that at minimum has an intermediate effect, or possibly substantive effect, with duration of, at minimum, days to weeks, if not longer. This leads to further define that society centric cyber conflict is a form of cyber conflict in which attackers cause at minimum intermediate disruptions or destructions, if not substantive disruptions or destructions, from which it will at least takes days to weeks, if not

[5] Healey et.al. (2020) focus on the duration and time needed to return to essential functions in the cyber domain. We argue that this scale can also be extended as framework to analyze the impact on attacks against critical infrastructure targets. I.e., how long before infrastructural targets hit by an attack can regain their functionality.

longer to recover, by attacking critical infrastructure targets that are essential for the (well) functioning of societies.

We believe this type of conflict can emerge via two routes. First, in what we refer to as the deliberate route, societal level cyber-attacks and conflict emerge as part of larger (interstate) (international) political conflict. Examples of these are the Russian cyber-attack on the Ukrainian power grid, or the recent Chinese attack on the Indian power grid. Both attacks had a clear societal impact – disruption of the power grid – and were conducted as part of larger international political conflict. In these cases, state actors deliberately attack critical infrastructure targets, and aim to cause a societal impact to influence adversaries' populations. Here we argue the aim of such societal level cyber-attacks is (among others) to influence public opinion and such political dynamics. The second route, which we refer to as the accidental route, is via societal attacks that are not part of any (larger) international political conflict but are singular stand-alone attacks that are (often) have a criminal purpose. Examples of such are the ransomware attack against the Colonial Pipeline that took place in May this year. While these attacks have no deliberate clear political purpose and do not deliberately seek to influence public opinion, they could as a result of their societal impact have (accidental) political implications: Societies under attacks and suffering from societal impacts could desire a forceful response by their governments. In both cases, as a result of the societal impact the public opinion would become a variable of importance in defining these governmental responses.

As a result, we argue that in the analysis of society centric cyber conflict the (possible) reaction and role of society should be essential. To date, because of the limited number of societal-level cyber attacks, we have a minimal understanding on the perception, role, and influence of societies on the dynamics of cyber conflict. Much of the recent analysis on cyber conflict views it either through a technical or IR lens, with societal factors having only a limited influence on the debate on the future of cyber conflict. However, we argue that if cyber-attacks increasingly will affect societies, it is imperative that we aim to better understand how societies could react to such attacks. Rovner (2021) illustrates how currently only a vague understanding exists on how societies could and would react. Indeed, what will happen if societies become subject to societal level cyber attacks? How will societies react to cyberattacks that disrupt and interrupt (possibly even destruct) societal life? The absence of clear understanding warrants more than sufficient reasons to conduct further research on society centric cyber conflict and the public's role in it.

2. Understanding the escalatory possibilities of society centric cyber conflict.

One of these essential issues that demands further study of societal-level cyber conflict and the population's role in this is the escalation potential of society centric cyber conflict. What kind of influence societies (that are subject to societal level attacks) have on this escalation potential? Would they favor escalations, and if so under which conditions, and to which extent? Or would societies prefer a de-escalatory approach? Rovner (2021) for example argues that interruptions to society's functioning and threatening the social order via cyber means could invoke strong desires among the public to pressure its political leadership to seek a settlement in conflicts. In this scenario, state populations would react in a de-escalatory manner, forcing political leaders to scale down any potentially violent responses. But what if the public opposes attempts at de-escalation? The Blitzkrieg and the bombing of German cities during WWII serve as a profound reminder of the resilience of societies facing aggressive pressure tactics. What if populations react the opposite way, and demand a robust and forceful response, possibly even with conventional military means against an adversary? In such a scenario, societal level cyber-attacks could increase the chances that the conflict dramatically widens.

Could populations subject to society centric cyber conflict bring nations closer to the brink of conventional war? These narrative builds on the assumption that society demands a more robust response because of the societal impact of such cyber-attacks, thereby increasing the escalation potential, including the possibility that such cyber conflict could evolve into conventional military conflict in the physical domain. This assumption builds on the argument that we should not look at the means of such an attack – cyber – but rather at the effect such cyber attacks cause: large scale harm or severe damage that causes disruptions and destructions that limit, pause, or cease critical functions of (a) society. In this, such cyber-attacks are little to no different in their intended effects from conventional offensive military operations, short of war (Farrell and Glaser, 2017; Kreps and Schneider, 2017). If the effects of such attacks are similar to the effect of conventional military operations, the argument can be advanced that they will follow the dynamics of conventional conflict escalation (Kreps and Schneider, 2017, p.3). If such cyberattacks cross the threshold from low-level temporary impairment, as they were previously, to permanently disruptive or destructive intensity, including physical harm and death, the potential for conflict escalation, including beyond the cyber domain, should significantly increase. The US cyber doctrine, for example, states explicitly that it foresees the right to strike back with conventional weapons, including nuclear, if a cyberattack has a significant negative impact for society as a whole. Following this logic, the new normal of societal-level cyber attacks could indeed significantly increase the potential for conflict escalation, well beyond the cyber domain.

However, this kind of logic might not be as clear-cut as some of the existing literature points out. As Kreps and Schneider (2017, p.3) note, "there is very little scholarly consensus about cyber escalation." Valeriano and Maness (2015), in their examination of the impact of cyber conflict on international interactions, and as such potential escalation, note the same problem as "few have endeavored to investigate the consequences of these actions" (Valeriano and Maness, 2015, p.302). Kreps and Schneider (2017) paraphrase Nye (2017, p.79), who argued that "[cyber] escalation ladders and thresholds are poorly understood." Nye (2017, p.70) contributes this to the absence of empirical evidence, yet simultaneously makes the case that when nuclear technology was introduced as a tool of warfare, it did not stop the emergence of theoretical debate on nuclear conflict and escalation potential. Nearly three years after Nye's article, some limited empirical evidence has now emerged. However, to the limited extent that such societal level cyber-attacks with physical impact have in fact occurred, no significant escalation has been witnessed (Healey and Jervis, 2020). With the minimal number of cases available for study, the debate on cyber escalation has taken place primarily in the theoretical realm. Valeriano and Maness (2015, 2018) and Borghard and Lonergan (2019) argue that escalation beyond the cyber domain remains unlikely for strategic and operational reasons, with conflict mainly taking place within the cyber domain, on the tit-for-tat level. Healey and Jervis (2020) illustrate that no escalation into the conventional military domain has actually taken place, yet in their paper come to a different conclusion and argue that depending on scope conditions - certain geopolitical conditions circumstances - escalation potential may be evident.

We argue that this debate should include now also include societal dimensions as a variable that influences the potential for conflict escalation in the cyber domain and beyond. What if societies demand robust reactions? We argue that in society-centric cyber conflict it is necessary and imperative to get to understand the role of the public. The argument that the public plays a significant role in the decision to escalate a conflict and even go to war, is best illustrated by Howard (1979). In his famed essay "The Forgotten Dimensions of Strategy," Howard illustrates the importance of social-political dynamics and public opinion on escalatory behavior and patterns and military conflict (Howard, 1979, pp.977, 982,984). While Howard focuses on potential nuclear conflict giving rise to military conflict in the nuclear era, we argue that his argument can, and should be extended to the current situation as well. With societal-level cyber-attacks having a similar effect, impact, and consequences as Howard's conventional military conflict dynamics, it seems equally apt to extend his argument to the role of the public and its bearing on conflict escalation. Omitting the public's perception and reaction from societal-level cyber conflict escalation would omit an essential variable in this process. Howard argues that the "compliance with […] public opinion became an essential element in the conduct of war" (Howard, 1979, p.977). In our opinion, such was the case in 1979 and before, and still is the case today. Thus, it is imperative that we study the role and influence of the public on the escalation potential of society-centric cyber conflict.

3. The possibility of society-centric cyber conflict in Asia.

While there have been global instances of societal-level cyber-attacks and society-centric cyber conflict, we are foremost interested in understanding the possibility of society-centric cyber conflict in the Asian region. This is for the following reasons; First, we are a research center based in this region and with a mission to highlight research from the region. Therefore, we believe it is logical that our attempt to understand the society-centric cyber conflict in praxis should geographically focus on this region. Second, the region is subject to several political, security, and military dynamics that ensure it is an ideal case study to understand if society-centric cyber conflict will further emerge, under which conditions, and its impact on regional political and security relations. As we argued prior in this paper society centric cyber conflict emerges via two different routes. Either of these presented itself in the region and could occur again. The first route – which we referred to as the deliberate route – has taken place already with the Chinese “Red Echo” attack against the Indian power grid (Recorded Future, 2021). Furthermore, throughout the region, numerous political conflicts exist, from the Taiwan Strait issue to the South and China Seas conflicts, the Sino-Indian conflict, the North-South Korea conflict, North Korea, and Japan, to a name a few. These conflicts have seen an increase in tensions, and the consensus among experts is that further increases are also likely. Under these conditions, actors might seek to use cyber means to send political signals. In particular, if actors would either seek to engage in acts of signaling or aims to influence an adversaries’ public opinion through the use of societal-level cyber-attacks. The use of such tactics would fit in the tactics of grey-zone conflict and salami-slicing, which is used widely in the region (Burgers and Romaniuk, 2019).

The potential for the accidental route also exists: North Korea has become a thriving offensive cyber actor that uses cyber-attacks for a monetary gain against all possible targets. This includes targets that are part of the earlier defined critical sectors. The example of the WannaCry attack has illustrated how North Korean hackers and its government have minor qualms about hitting targets that are part of critical infrastructure. The interruptions caused by such attacks have only been disruptive, with slight impacts and minor effects. However, in target rive environment, as exists in the region where cybersecurity standards are often faulty and inadequate, North Korean ransomware attacks and other offensive-for-monetary-purposes attacks will likely hit critical infrastructure sectors, with a potential for attacks with accidental significant or decisive effects, triggering a societal impact and reaction.

The sum of this illustrates that there is a significant possibility that societal-level cyber-attacks and society-centric cyber conflict will emerge. Given this, and in combination with our research, we believe the Asian Pacific region offers itself a worthwhile case study to understand how society-centric conflict emerges, develops, its potential for conflict escalation, and how it relates to and influences conventional security relations and dynamics.

4. Methodological approach to gather research data.

To understand the public's perception of and measure the impact of societal-level cyber-attacks and to study society-centric cyber conflict, we have decided to use surveys as a tool to gather the necessary data on the public's perception and reaction. However, the absence of sufficient data has led to consider another methodological approach with surveys arising as the most feasible and economically viable opportunity to gather data. Therefore, a survey was developed by the Cyber Silent Spring team, executed by a market research firm in China, Japan, South Korea, and Taiwan. Using fictive scenarios, we sought to understand each of the nations' societies thinking on societal-level cyber-attacks and society-centric conflict. Our survey used five different cyber-attack scenarios – with an increasing societal impact – and give respondents six reaction choices, with an increasing escalatory effect, to determine how and by what means respondents would react. The survey aimed to determine a) how citizens would react, b) by what means, and c) and if the variable of disruptive or destructive effect matters in the public's response. This should enable us to learn if

1. how societies think about societal-level cyber attacks,
2. how they would react when subject to such attacks,
3. if societies would seek escalatory or de-escalatory responses, if so by what means, and
4. how this influences (broader and conventional) political and security relations.

5.Conclusion

This paper discusses the rise of society-centric cyber-attacks and society-centric cyber conflict. We focus on the recent phenomena of cyber-attacks that deliberately target critical infrastructure and potentially affect societies and their societal functions directly. Our framework illustrated that not all attacks have societal impacts but rather that this depends on the target and the efficacy of such attacks. These define if these attacks will have a societal impact and to which extent. We argue that cyber-attacks with a societal-level impact lead to what we refer to as society-centric cyber conflict: A form of cyber conflict in which attackers cause at minimum intermediate disruptions or destructions, if not substantive disruptions or destructions, from which it will at least takes days to weeks, if not longer to recover, by attacking critical infrastructure targets that are essential for the (well) functioning of societies.

We differentiate between society-centric cyber attacks that have deliberate and accidental societal impact attacks and argue that while different in initial intentions, both lead to societal reactions. As societies are directly affected and interrupted in their functioning, we expect that societies demand a voice in governmental responses to such attacks. Their influence shapes how governments react to such attacks, with our specific interest in understanding how societal reactions affect the escalatory potential of cyber conflict. Understanding these dynamics is, in particular, relevant for Asian Pacific: A region where societal level cyber-attacks are emerging.

To further advance our research on this, we have conducted surveys in East Asia. The survey data should enable us to measure societal impact, allowing us to proceed to the next step of this research project, which is a) to understand the correlation between the societal impact of attacks and societal reactions and b) how societal reactions affect the dynamics of society centric cyber conflicts and its escalatory potential.

6.References.

Borghard, E. D., & Lonergan, S. W. (2019). Cyber Operations as Imperfect Tools of Escalation. *Strategic Studies Quarterly*, *13*(3), 122–145.

Bumiller, E., & Shanker, T. (2012, October 11). *Panetta Warns of Dire Threat of Cyberattack on U.S.* The New York Times. https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html.

Council of the European Union. (2008). *COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection* (pp. L 345/75-L 345/82) (European Union, Council of the European Union, Council of the European Union). Brussels, EU: Official Journal of the European Union.

Cybersecurity and Infrastructure Security Agency (CISA). (2020, October 21). Critical infrastructure sectors. Retrieved July 24, 2021, from https://www.cisa.gov/critical-infrastructure-sectors

Cybersecurity Strategic Headquarters. (2017, April 18). *The Cybersecurity Policy for Critical Infrastructure Protection* (Japan, National center of Incident readiness and Strategy for Cybersecurity, Cybersecurity Strategic Headquarters). Retrieved July 24, 2021, from https://www.nisc.go.jp/eng/pdf/cs_policy_cip_eng_v4_r2.pdf

Farrell, H., & Glaser, C. L. (2017). The role of effects, saliencies and norms in US Cyberwar doctrine. *Journal of Cybersecurity*, 1–11. https://doi.org/10.1093/cybsec/tyw015

Glosserman, B. (2020, June 10). *A 'new normal' in cyberwar should scare us to action*. The Japan Times. https://www.japantimes.co.jp/opinion/2020/06/10/commentary/world-commentary/new-normal-cyberwar-scare-us-action/.

Goldman, E. O. & Warner, M. (2017). Why a Digital Pearl Harbor Makes Sense . . . and Is Possible. In Perkovich, G. & Levite, A.E. (Ed.), *Understanding Cyber Conflict: Fourteen Analogies*. https://carnegieendowment.org/files/GUP_Perkovich_Levite_UnderstandingCyberConflict_Ch9.pdf.

Greenberg, A. (2019, November 5). *The Story of Sandworm, the Kremlin's Most Dangerous Hackers*. Wired. https://www.wired.com/story/sandworm-kremlin-most-dangerous-hackers/.

Greenberg, A. (2019, October 17). *Inside Olympic Destroyer, the Most Deceptive Hack in History*. Wired. https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/.

Healey, J., Jenkins, N., & Work, J. (2020). Defenders disrupting adversaries: Framework, dataset, and case studies of Disruptive Counter-cyber operations. *20/20 Vision: The Next Decade2020: 12th International Conference on Cyber Conflict (CyCon),* 251-274. doi:10.23919/cycon49761.2020.9131725

Healey, J., & Jervis, R. (2020). The Escalation Inversion and Other Oddities of Situational Cyber Stability. *Texas National Security Review*, *3*(4), 31–53.

Herbolzheimer, C. (2016, September 14). *Preparing for a Black Swan Cyberattack*. Harvard Business Review. https://hbr.org/2016/09/preparing-for-a-black-swan-cyberattack.

Howard, M. (1979). The Forgotten Dimensions of Strategy. *Foreign Affairs*, *57*(5), 975–986. https://doi.org/10.2307/20040266

Jhangiani, T., & Kennis, G. (2021, June 15). Protecting the critical of critical: What is systemically important critical infrastructure? Retrieved July 27, 2021, from https://www.lawfareblog.com/protecting-critical-critical-what-systemically-important-critical-infrastructure

Kreps, S., & Schneider, J. (2019). Escalation firebreaks in the cyber, conventional, and nuclear domains: moving beyond effects-based logics. *Journal of Cybersecurity*, *5*(1), 1–11. https://doi.org/10.1093/cybsec/tyz007

Lawson, S., & Middleton, M. K. (2019). Cyber Pearl Harbor: Analogy, fear, and the framing of cyber security threats in the United States, 1991-2016. *First Monday*, *24*(3). https://doi.org/10.5210/fm.v24i3.9623

Levite, A. E., & Shimshoni, J. Y. (2018). The Strategic Challenge of Society-centric Warfare. *Survival*, *60*(6), 91–118. https://doi.org/10.1080/00396338.2018.1542806

Maness, R. C., & Valeriano, B. (2015). The Impact of Cyber Conflict on International Interactions. *Armed Forces & Society*, *42*(2), 301–323. https://doi.org/10.1177/0095327x15572997

Nye, J. S. (2017). Deterrence and Dissuasion in Cyberspace. *International Security*, *41*(3), 44–71. https://doi.org/10.1162/isec_a_00266

Perlroth, N., & Krauss, C. (2018, March 15). *A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try.* The New York Times. https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html.

Recoded Future. (2021). *China-Linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions*. Recorded Future. Retrieved from https://go.recordedfuture.com/hubfs/reports/cta-2021-0228.pdf?utm_medium=email&_hsmi=110851062&_hsenc=p2ANqtz-_fR2eW1z1fseEubXquIBbiMBtpgOMFQHoO8FSSYMRPL22HRfOlQRJJgcrcKE-qqnaIppBfht_CCEdLSpqpmc5ymvrfBkm_xpWqt3ZbbD6xYuza9cc&utm_content=110851062&utm_source=hs_automation

Rogers, Z. (2019, June 4). *Have Strategists Drunk the "AI Race" Kool-Aid?* War on the Rocks. https://warontherocks.com/2019/06/have-strategists-drunk-the-ai-race-kool-aid/.

Rovner, J. (2021, March 17). *Warfighting in Cyberspace*. War on the Rocks. https://warontherocks.com/2021/03/warfighting-in-cyberspace/.

Schneider, J. (2020, January 7). *It's Time to Calibrate Fears of a Cyberwar With Iran*. The New York Times. https://www.nytimes.com/2020/01/07/opinion/iran-cyber-attack-hacking.html.

Valeriano, B., & Maness, R. C. (2018). How We Stopped Worrying about Cyber Doom and Started Collecting Data. *Politics and Governance*, *6*(2), 49–60. https://doi.org/10.17645/pag.v6i2.1368