2020 12th International Conference on Cyber Conflict
20/20 Vision: The Next Decade
T. Jančárková, L. Lindström,
M. Signoretti, I. Tolga, G. Visky (Eds.)
2020 © NATO CCDCOE Publications, Tallinn

Correlations Between Cyberspace Attacks and Kinetic Attacks

Martin C. Libicki
Distinguished Visiting Professor
Center for Cyber Security Studies
U.S. Naval Academy
Annapolis MD, USA
libicki@usna.edu

Abstract: Although confrontations in cyberspace can conceivably stay in cyberspace (or at least not involve violent conflict), they can also become entangled with confrontations in the physical world. This paper explores how, by raising the following questions: (1) Do countries retaliate in the real world for operations in cyberspace? (2) Would countries make an equivalence between the damage from cyberattacks and from physical attacks (in ways that could spill over from the one to the other)? (3) Does cyberspace escalation lead to kinetic escalation and is the reverse also true? (4) Can cyberspace operations against sensitive targets put them in play for kinetic operations? (5) Would the failure to react to cyberattacks embolden attackers to carry out kinetic attacks? This paper leverages what is known and what can be logically assumed about cyber operations, notably by drawing lessons from Russia's use of cyberspace operations in Georgia and Ukraine, Iran's cyber and physical attacks against Saudi Aramco, and China's military doctrine vis-à-vis U.S. space assets. The broad conclusion is that, so far, conflict in cyberspace rarely echoes into the world of kinetic conflict (although kinetic conflict increasingly has cyberspace dimensions). This raises the question of whether and why a threshold is emerging between non-lethal and lethal attacks.

Keywords: *escalation, cyberattack, kinetic*

1. INTRODUCTION

Although interstate confrontations in cyberspace *could* stay in cyberspace (or at least within the information domain), nothing mandates that both sides will observe such boundaries. Cyberattacks can become entangled with more conventional military operations, as they have in Georgia (2008) and Ukraine (2014-).

If this is true, *the prospect that conflict in cyberspace can bleed over into kinetic conflict suggests that operations in cyberspace have the potential to cause more serious instability than assumed* (e.g. Healey 2019). But, is it true?

To explore the issue, we look at the relationship between incidents and escalation in cyberspace and their counterparts in the physical world by posing five sub-questions:

- Do countries retaliate in the real world for operations in cyberspace?
- Would countries make an equivalence between the damage from cyberattacks and from physical attacks (in ways that could spill over from the one to the other)?
- Does cyberspace escalation lead to kinetic escalation and is the reverse also true?
- Can cyberspace operations against sensitive targets put them in play for kinetic operations?
- Would the failure to react to cyberattacks embolden attackers to carry out kinetic attacks?

We will try to use (known) past events to address these questions. That said, there are not many incidents to work with. Although scholars have compiled large datasets of cyberspace incidents (see, in particular, Valeriano, Jensen, and Maness 2008), the bulk of them, by far, are acts of cyberespionage, and many of the rest are Distrubuted Denial of Service (DDOS) attacks. The paucity of examples relevant to escalation necessarily limits how robust any answers are to future events.

2. DISTINCTIONS AND CAVEATS

Despite the prominence of "persistence" as reflected in the phrases "advanced persistent threat" or "persistent engagement", conflict in cyberspace tends to have an episodic quality. There is no good equivalent to holding or contesting land (persistent access to a system is only slightly analogous). Incidents of cyberspace conflict are often *sub rosa*, and usually unacknowledged. They have not followed declarations of war or any of its modern equivalents. As a practical matter, it is hard to judge whether

any one cyberspace operation – especially one in a long series of similar events – is or is not escalatory.

Escalation, itself, has been defined as "an increase in the intensity or scope of conflict that crosses threshold(s) considered significant by one or more of the participants" (Morgan et al. 2008). This formulation contains two key elements.

One element is the ability to measure the *intensity* of cyberspace operations. This requires, at a minimum, two such operations of a similar type between the same combatants and in the same or similar context – plus some metric that indicates that one is more serious than the other. But intensity is a measure of effort, not success. It has to be inferred from a set of incidents whose effects reflect not only intensity but other factors such as the quality of defense. In other words, while one side may have increased the intensity of its efforts, the other side may not perceive as much if its defenses have risen to the challenge. Perhaps the best that can be said of a cyberattack is that it may be considered akin to escalatory if it is unexpected or at least unprecedented in a particular context.

A second element in the definition is the existence of significant thresholds. It is unclear whether there are *any* such thresholds in cyberspace, *per se*. There is no broad consensus as to what targets are off limits. In 2015, the UN Group of Government Experts tried to put civilian infrastructures off limits (United Nations 2015), but power grids *have* been attacked by at least one great power since then (Goodin 2015 and 2017). Putatively, there may also be a recognized threshold between a cyberattack with casualties and one without. But no cyberattack has caused direct casualties and determining indirect casualties is difficult. Indirect casualties are subject to dispute: e.g., do two reported suicides after exposing the customers of the Ashley Madison website count (Baraniuk 2015)? Even if Wannacry was associated with higher-than-expected death rates in U.S. hospitals, the details are hidden in litigation and a close review of death rates in Britain's National Health Service shows no discernable net effect (Ghafur et al. 2019). Although the definition of escalation may be fulfilled if one side (typically, the target) believes that a cyberattack has crossed the line, countries have been slow to determine or at least announce what such lines might be. Calling a cyberattack escalatory if it produces unexpected (and, generally, more severe) consequences may be close enough to right.

A third element is the challenge of determining whether one attack was a response to another. This is particularly difficult in cyberspace, where a cyberattack carried out as a response may require establishing accesses in a target system, a process of hard-to-predict length. In some cases, it may require establishing a capability; Iran could

not respond to Stuxnet in 2010 until it had built capabilities that it deployed in 2012. However, generating a *kinetic* response to a cyberattack would seem to take less time.

One last caveat. In physical combat there is a *rough* correspondence that relates effort to effects and effects to perceptions (of effects) – despite the fog and friction of war or the difficulties of battle damage assessment. Time creates the opportunities to sort out much of what initially appears ambiguous. In cyberspace, most probes fail, many go unnoticed, and even successes are not always immediately discovered. Stuxnet, for example, which clearly destroyed Iranian centrifuges, was not detected as a cyberattack until the summer of 2010 even though its effects took place in late 2009 and early 2010. Only later did Iranians come to understand that the failures they were definitely seeing resulted from deliberately corrupted commands rather than accidents, poor operational procedures, or substandard components. Malware implants present a particular problem. Finding one in a target system may offer little indication of what its purpose was: e.g., espionage or cyberattack? If the purpose is obscure, the intent will be at least as obscure. This leaves in doubt whether the other side intended to escalate. And even a more fully-completed cyberattack which shows that, say, a system's controls can be usurped, does not prove whether the point was to test procedures, brandish capabilities, or wreak damage. Arguably, the late 2016 Russian cyberattack on the Ukrainian power grid was deliberately stopped once the point was made, when it could have gone far longer (Greenberg 2019). Again, we can only work with what we have. This may explain why the topic can use further exploration despite good conceptual work having been done (Borghard and Lonergan 2017; Lin 2012).

3. PROPOSITION: CYBERATTACKS CAN LEAD TO KINETIC RETALIATION

Were this true, then a sufficiently grave cyberattack could have serious escalatory consequences by crossing the boundary into what is commonly recognized as armed conflict. In 2009, an anonymous U.S. administration source asserted that "If you shut down our power grid, maybe we will put a missile down one of your smokestacks" (Gorman and Barnes 2011). Accordingly, a cyberattack would beget kinetic retaliation, which begets more kinetic retaliation, which evolves into a war, and, if at least one side has nuclear weapons, a chance, albeit very small, of nuclear Armageddon.

Nothing *so far* suggests this as a plausible scenario. True, small-scale tit-for-tats in cyberspace (mostly web defacements and DDOS attacks) have taken place between the usual dyads (e.g., India and Pakistan or Israel and Palestinians). But the only significant retaliation for a cyberattack – and not everyone sees it that way – has been

the Iranian DDOS attacks on U.S. banks in late 2012 as a response to the Stuxnet attack of 2010 and (with somewhat less clarity) Iran's use of wiper malware against Saudi Aramco and Qatar after a similar wiper attack on its refineries (Zetter 2015).

The shift from cyberattacks to violent attacks has so far been scarce and ambiguous. One *possible* incident was the violent death of Mojtaba Ahmadi, the commander of Iran's Cyber War Headquarters, several weeks after the traffic controls of Haifa's Carmel Tunnel had been hacked (see InfoSecurity 2013; McElroy and Vahdat 2013). Even though the cyberattack preceded the death, Israel's announcement came afterwards. Both Israel and Iran deny the connection, however. Another was a physical attack on a Gaza building said to house Hamas hackers – but such claims could be dismissed as an opportunistic justification of a particular bombing attack, carried out during a conflict in which bombing attacks of all sorts were frequent (Chesney 2019).

Conclusion: a kinetic retaliation to a cyberattack is possible but cannot yet be deemed a likely consequence.

4. PROPOSITION: CYBERATTACKS WILL BE TAKEN AS SERIOUSLY AS EQUALLY DAMAGING KINETIC ATTACKS

If countries react to cyberattacks as they would to equivalent kinetic attacks, then an escalation in cyberspace (defined as above) could well result in a comparable escalation in physical space – again with the expected effects on international stability.

But would they? Much of the answer depends on what constitutes "comparable." Kinetic military effects tend to include death and destruction. No cyberattack has killed anyone directly, and few have actually broken physical things; wiping a hard drive – as many cyberattacks have done – still leaves the hard drive physically intact. But cyberattacks have been quite costly to their victims, even if measured solely in disruption and remediation costs. The NotPetya attacks were said to have cost their (mostly corporate) victims up to $8 billion (Greenberg 2018). Putatively, a kinetic attack that destroys $8 billion worth of military equipment but harms no one would be comparable and should, one would imagine, bring about a comparable reaction.

Imagining a kinetic attack that breaks things but hurts no one used to be an exercise in fantasy. But the Iranian take-down of a $150 million U.S. Global Hawk in the summer of 2019 *was* such an attack. The U.S. response, a cyberattack, was also non-lethal. Lest this choice of avoiding lethality be ascribed to the individual characteristics of the U.S. President, note that the Pentagon was also thinking along similar lines. One

of its favored options was to sink an Iranian craft, but only *after* giving its sailors time to get away (Baker, Schmitt, and Crowley 2019). Earlier, a Turkish shootdown of a Russian jet near the Syrian border had drawn a cyber response (e.g., DDOS attacks), but nothing violent (Murgia 2015).

Returning to NotPetya, the U.S. reaction to this costly event was a limited set of sanctions. If Russia had deliberately disabled commercial satellites whose total replacement value summed to that much, would the United States have also limited its response to sanctions? One might counter that many of the affected corporations were not U.S.-headquartered: for example, Maersk, a Danish shipping company. If that matters, then replace United States by NATO and re-ask the question. So, while the non-lethality of cyberattacks means that a plausible response would be non-lethal, the failure to respond to NotPetya suggests that the broad scope of the cyberattack may have also played a role. Perhaps a cyberattack that damages software and thereby levies costs on victims is different in kind from a comparably costly kinetic attack that damages hardware.

Research by Professor Jacqueline Schneider casts further doubt that a cyberattack would be treated as tantamount to a comparable kinetic attack (see Kreps and Schneider 2019). The results of two exercises – one conducted at the U.S. Naval War College and the other on-line – suggest that cyberattacks introduced into a simulated crisis were more often ignored or, at most, motivated a weak response in comparison to comparable kinetic attacks.

In fairness, the United States has been used as the exemplar of how countries may respond to cyberattacks and other countries may react differently. But the United States deserves attention because it has responded most overtly, whether through public statements, levied sanctions, or news reports (Israel is also active, but it is a far smaller country and unique in many relevant respects). It is unclear whether the difference is that the United States suffers more cyberattacks than other countries (or seems to in part because of uncensored media coverage) or whether other countries have covert ways of responding that are not widely known. That noted, Jensen and Valeriano (2019) indicate that when citizens of the United States, Russia, and Israel were given a scenario with a major cyberattack, only a small percentage chose to escalate as a result. Roughly half of the respondents wanted something less than a tit-for-tat response. They concluded that, "to date, cyber operations have tended to offer great powers escalatory offramps".

Conclusion: cyberattacks would be deemed less likely to garner a kinetic response than would kinetic attacks that levy comparable costs, because they are generally non-lethal and somehow considered less serious and more easily recovered from.

5. CYBERATTACKS PRESAGE KINETIC ATTACKS

An opening attack by a country that is adept at cyberattacks against a country that depends on information systems could be a precursor to a broader armed attack. Cyberattacks, especially against a surprised – hence unprepared – target, have some potential to blind, confuse, and even disarm the adversary, making conventional victory easier. Cyberspace theorists from James Mulvenon onward have posited a Chinese military campaign whose first move is to paralyze the U.S. ability to move warfighters and materiel across the Pacific, giving China additional time to take and consolidate military objectives in East Asia before the United States arrives in force. One advantage of using cyberattacks this way is that the ambiguity about their characteristics (while the target asks: why are systems failing?) and their attribution can retard the target's conclusion that it must prepare for immediate war. By contrast, a kinetic attack (e.g., against sensors) initiated as a prelude to wider hostilities would more certainly remove the element of surprise when the wider hostilities commenced.

The best case that cyberattacks do precede kinetic attacks comes from the Russia-Georgia war in 2008. Just prior to the onset of that conflict (dating from when Russian troops moved into Georgia and not into South-Ossetia, a part of Georgia outside its government's *de facto* control), DDOS attacks from Russian sources (probably but not provably state-directed) limited Georgia's access to the Web, notably preventing the government from putting out its view of the conflict. Russian cyber or at least electronic interference may have deliberately hindered Georgia's mobile phone system, which had military uses. By contrast, Russian DDOS attacks on Estonia (which may or may not have been state-directed) *followed* the first night of riots by ethnic Russians in Tallinn (April 26, 2007) which themselves were prompted by Estonia's decision to move the "Bronze Soldier" from downtown to a nearby military cemetery. And these DDOS attacks did not precede any kinetic military operations by Russia against Estonia.

Cyberattacks – with the important exception of DDOS attacks – typically require months of planning. Unpredicted kinetic conflicts are thus unlikely to be preceded by cyberattacks. In 2011, NATO aircraft were engaged over Libya, and the threat that they would be shot down by Libyan surface-to-air missiles (SAMs) reportedly prompted discussion of using cyberattacks to neutralize these SAMs (Nakashima 2011). Ultimately, no such cyberattack took place (as far as publicly revealed). By the time it could have been completed, there would have been little need to suppress Libyan SAMs. If NATO had anticipated in advance having to fight in Libya – riots in Tunisia that set off the Arab Spring did precede NATO operations over Libya by three months – it might have had time to disable Libyan SAMs by cyberattack, but hindsight never needs glasses. Conversely, if cyberattacks *are* used to precede kinetic

combat, or even in the first days of kinetic combat – and their effects are detected and correctly attributed – then it would be difficult for the cyberattacker to claim that war had been a complete surprise to it. The timing of events would suggest that the cyberattacker had assessed the possibility of war as being likely enough to justify laying in cyberattack preparations. This would strain any argument that the target (of the cyberattacks) had started the war out of the blue.

In a putative future in which every major country has implants in the military systems of anyone they have the remotest chance of having to fight against, then a cyberattack may not be so indicative. But that has (probably) not yet happened. What is likely to come first is that major countries will be distributing implants into adversary networks for cyberespionage – which, after all, is a normalized peacetime activity that friends do even to friends. But though, in theory, every cyberespionage penetration is a potential cyberattack penetration, the immediate targets will be different. Because the knowledge possessed by SAM systems has limited intelligence value, such systems are rarely first-tier targets for cyberespionage. As a rule, the knowledge necessary to cause specific types of failures (e.g., how to make a centrifuge spin itself to death) must be acquired specifically for that purpose. If reports are reliable, however, the United States *has* placed implants in the military systems of countries it may have to fight. The aforementioned Iranian shootdown of a Global Hawk missile was, ultimately, followed by a U.S. cyberattack on Iran's ship-tracking database. In all likelihood, the path to the database was laid in *before* Iran shot down the Global Hawk (mid-June 2019) and may have been laid in even before Iran (re)started targeting commercial shipping (mid-May 2019) – although if Iran's networks were easy to penetrate, preparatory intrusions could have started not much earlier than the cyberattacks did. Before the Joint Comprehensive Plan of Action (JCPOA) agreement of 2015 with Iran, there were stories that the United States had laid in attacks against Iranian electrical infrastructures named *Nitro Zeus* (Sanger and Mazzetti 2016).

In the conflict between Russia and Ukraine, most of the major cyberattacks have come from Russia. Because the war would not have started but for the unexpected resignation of Ukraine's President Viktor Yanukovych, Russia did not accompany its kinetic operations with cyberattacks that required great planning – although it did carry out DDOS attacks and acts of electronic warfare from its outset. Over time, Russians did attack Ukraine's infrastructure and launched a notable supply chain attack (from whence NotPetya) against the Ukrainian company, MeDoc. But the attack on Ukraine's power grid did not take place until the second year of conflict. Detailed study of the Ukraine and Syria conflicts suggests that "cyber activities failed to compel discernible changes in battlefield behavior. Indeed, hackers on both sides have had difficulty responding to battlefield events, much less shaping them" (Kostyuk and Zhukov 2017).

There are no known examples, however, of the *target* of a surprise kinetic attack having pre-empted such an attack using cyberattacks.

Conclusion: although most cyberattacks do not presage kinetic combat, some cyberattacks might. Surprise cyberattacks by a cyberspace-adept country against a cyberspace-dependent country would offer the best opportunity for their usage, but many kinetic wars come as a surprise to both sides.

6. PROPOSITION: CYBERATTACKS MAY PUT HITHERTO SACROSANCT TARGETS IN PLAY FOR KINETIC ATTACKS

In WWII, cities were initially considered sacrosanct. Then Germany bombed Warsaw and later Rotterdam, but these targets could be considered of direct relevance to military operations on the ground. Then Germany bombed residential districts of London while allegedly going after air defense sites. Then both sides practiced unrestricted air warfare. Today, there is a broad, but not necessarily realistic, expectation that space systems and nuclear command-and-control systems are sacrosanct. One can easily imagine a conflict, perhaps one of local relevance only, in which such systems are initially considered off limits by both sides – only to be placed in-bounds by subsequent escalation. Such escalation may have many sources, but one potential source is that cyberattacks on space and/or nuclear command-control-and-communications (NC3) systems may put targets in play for kinetic attacks as well.

Space systems and NC3 systems really ought not to be accessible to cyberattack. Their military criticality should make anyone think twice about connecting them to the outside world, and they do not need the Internet to function. But these circumstances hardly provide proof against mischief – for the usual reasons. Not everyone understands how the fact of access alone heightens cybersecurity threats. The pressure to expand access to sensitive systems is often hard to resist, especially when expanding access can facilitate their support and maintenance. Not every access point is easy for defenders to discover; some system components have been given unadvertised connectivity at the factory or in the course of repair. People put great trust in protections (e.g., firewalls) that can be manipulated. So, while we lack documented evidence that any hacker has breached NC3 systems, it is too early to say for sure that they cannot be hacked (Futter 2018). And while cyberattacks on *military* space systems have not been reported, probable hostile penetration of the control systems of civilian satellites has been (see Barrett 2019; Leavitt 2011; Newman 2018; Tucker 2019).

To be fair, it is unclear how sacrosanct space systems really are from *kinetic* attack anyway. The United States, China, Russia, and India have all tested anti-satellite systems. And while all four have paid respect to the notion of peace in the heavens, none has foresworn being the first to use their anti-satellite systems. Finally, satellites can be destroyed without creating casualties, an argument in favor of their being targeted if military need arises.

The inviolability of NC3 systems in scenarios short of nuclear war is based on the proposition that nuclear stability requires the major powers to be assured of their second-strike retaliatory capability. Some (Acton 2018) fear that cyberattacks on systems that support command-and-control for both conventional and nuclear systems will seem motivated to reduce the target's nuclear retaliatory capability in the guise of legitimate warfighting. Such suspicions could lead, at best, to twitchy adversaries apt to overreact to any further threat to their capability – and, at worst, to adversaries concluding that they must use their nuclear weapons before they otherwise lose them. Accordingly, others (Danzig 2014) have proposed that the major powers pledge not to carry out cyberattacks on adversary NC3 systems – a proposition that, suffice it to merely note, is both laudable and problematic: enforcement would be difficult and might require banning NC3-directed cyberespionage, some types of which could provide reassurance against surprise attack.

But will cyberattacks on space or NC3 systems put them in play for kinetic attacks among the immediate combatants – or worse, create a precedent that colors how every other country might treat its foes' systems? Maybe not – in part because of the ambiguity and the non-lethal nature of cyberattacks. Ambiguity affects three questions. *One*, were the perceived effects the result of adversary action – in contrast to misunderstandings (e.g., of how the supposedly targeted system was supposed to work), design flaws, accidents, Mother Nature, etc.)? *Two*, if adversary actions were the cause, were they deliberate, or inadvertent (e.g., because of hacker mistakes, malware drift, etc.)? *Three*, was the cyberattacker the same adversary that is attacking in physical space? The importance of determining why systems failed is clear enough. Whether or not system failure was *deliberate* speaks to the other side's intent, whether it was sending a signal, and whether a repeat performance can be expected. The importance and the difficulty of attribution is clear enough, as well. Time also plays a role. With the Pearl Harbor attack, to give an example, its fact, its deliberateness, and its perpetrator were instantly obvious. Characterization, intentionality, and attribution in cyberspace may also be instantly obvious in some cases, but in other cases could take time to discover. Reaching a conclusion that action is merited may precede acquiring 100% confidence in that conclusion – and it may take a great deal of confidence to escalate a conflict when there is some lingering doubt that any such escalation was

forced on the target. In the, say, months in-between, matters may escalate for other reasons – or the conflict could end.

The non-lethal and often temporary nature of cyberattacks may also put off comparable escalation into unleashing kinetic attacks on satellites. All possible satellite attack modes are non-lethal (with two minor exceptions: attacks on the International Space Station and attacks whose debris causes ground casualties). And many physical attacks on satellite services – such as jamming, dazzling, or blinding – are temporary and, as such, likely to be carried out before contemplating escalating to destructive attacks. By contrast, many attacks that destroy satellites can endanger all other satellites by create long-orbiting space debris. So, the best guess at this point is that cyberattacks on satellites with reversible effects would be treated like temporary physical attacks. Cyberattacks that disable satellites permanently (e.g., by directing them to an unsustainably low orbit) – and such permanence may take a while to ascertain – would be considered more serious but not as serious as physical destruction. But that does not mean that cyberattacks would be shrugged off.

NC3 systems include a wide variety of components. Some are unmanned: e.g., satellites (for communications, and early warning), radar dishes, communications lines, transmission towers. Others are manned: e.g., radar stations, command centers, command authorities (e.g., key nuclear commanders wherever they are). Many can be disabled by cyberattacks, but few can be disabled permanently that way. The range of temporary attacks on NC3 based on physical effects (e.g., as dazzling, jamming, or blinding are for satellites) is limited compared to the array available against satellites. Finally, kinetic attacks against many NC3 components risk casualties. Conversely, the sacrosanct nature of NC3 systems is better established than with satellites. Thus, a best guess at this point is that cyberattacks against NC3 systems – provided they are confidently characterized and attributed – can open the door for kinetic attacks against NC3 systems. A lot will depend on whether the two parties are fighting a kinetic war at the time. If so, a response may come faster. If not, a lot may depend on events that intervene before a next kinetic war starts.

Conclusion: cyberattacks have the potential to put privileged assets in play for kinetic attacks, but not necessarily.

7. PROPOSITION: FAILURES TO RESPOND TO CYBERATTACKS EMBOLDEN KINETIC ATTACKS

A failure to respond could mean (1) doing nothing, (2) doing something that falls short of signaling seriousness (e.g., imposing individual economic sanctions after NotPetya), or (3) doing something that should impress the attacker but does not. Here, we focus on the possibility of an unanswered escalation in cyberspace emboldening escalation in physical space by the same actor.

The evidence here is mixed.

In the ongoing undeclared conflict between Saudi Arabia and Iran, cyberattacks on Saudi Aramco in 2012 wiped the memories of roughly 30,000 computers. The same attack may have tried to ruin physical (oil field) equipment but never reached that far (Perlroth 2012). Putatively, this may have been retaliation for a less-well-reported cyberattack on Iran's main oil export terminal (Reuters 2012). Neither Saudi Arabia nor the United States retaliated (as far as known). In the summer of 2019, Saudi Aramco facilities were hit by missile attacks; by the end of 2019 there had been no kinetic response nor any other response (also, as far as known). Did the lack of response to the 2012 cyberattack therefore encourage Iran to think it could get away with a physical attack? Note that in both cases, attribution was not instant. The 2012 cyberattack initially looked as if it could have been an inside job, until the consensus formed that it was Iran's doing. The 2019 missile attack on Aramco refining facilities was initially ascribed to Yemen's Houthi rebels, although later analysis indicates that the discerned direction of the incoming missiles was unlikely if launched from Yemen and that the Houthi rebels anyway lacked the technological sophistication to aim their weapons so accurately. Indirectly, and perhaps even directly, it was Iran's doing. Although the failure to push back hard on Iran's earlier kinetic attacks on neutral shipping and the U.S. Global Hawk may have persuaded Iran it could have gotten away with the missile attack, the failure to see much response from their 2012 cyberattack may have played a role in such assurance as well.

The Russo-Ukrainian conflict featured multiple cyberattacks. The NotPetya malware was designed to undermine trust in the products of Ukrainian corporations. Electrical systems were hacked twice. However, there have been essentially no *kinetic* attacks on Ukrainian infrastructure (at remove from the front lines in eastern Ukraine). Thus, the general failure of the West to respond to Russian cyberattacks on infrastructure does not seem to have encouraged Russia to launch kinetic attacks.

Conclusion: there is scant evidence *so far* that a failure to respond to cyberattacks, especially on critical infrastructure, puts them in play for kinetic attacks.

8. OVERALL CONCLUSIONS

Overall, there is little public evidence that hostile events in cyberspace echo strongly outside it. Indeed, rarely do events in cyberspace – much less escalation in cyberspace – lead to serious responses at all. Some research suggests that even severe cyberattacks would generally be less likely than kinetic attacks to induce a response. Although opening cyberattacks can precede kinetic attacks, there are also cases when war comes as a surprise and cyberattacks are not used until the proper accesses to target systems have been gained. Cyberattacks have the potential to put hitherto sacrosanct targets – notably space systems, and other NC3 elements – in play, but cyberattacks have reportedly taken place against satellites while kinetic attacks (weapons tests aside) have not, so far. The failure to respond to cyberattacks *may* have played a role in enabling missile attacks on Saudi Aramco facilities, but the link is distant (seven years earlier) and tenuous. There is no analog (yet) in the Russo-Ukrainian conflict.

Several reasons could be adduced to explain the lack of correlation. One is that while there *could be* cyberattacks consequential enough to induce echoes in the physical world, none have reached that threshold and it may well be that none *could* reach that threshold. Even as the attack surface for cyberspace operations keeps growing, hackers grow more talented, and their leaders more aware of the gains available from such operations – defense is not sleeping. Those who own networks are taking cybersecurity seriously (at long last), cloud computing may have helped put defenses in the hands of those for whom protection is a profit center, and the cybersecurity industry itself is robust. Succeeding generations of software – e.g., versions of Windows operation systems – are also more impervious to intrusions. Two is that, in common with many widely-feared phenomena, cyberattacks have evolved from an acute problem (one both rare and fearsome) to a chronic problem (more common, but something that one can adjust to). Three, the oft-expressed belief that cyberwar is war has yet to take hold. Because cyberspace operations are ambiguous (and not easily grasped even when clear) and their effects almost always temporary and not (yet) lethal, they may be considered something separate and apart. Time will tell whether this distinction will continue to be observed.

REFERENCES

Acton, James. 2018. "Escalation through Entanglement." *International Security* 43, no. 1 (Summer): 56–99.

Baker, Peter, Eric Schmitt, and Michael Crowley. 2019. "An Abrupt Move That Stunned Aides: Inside Trump's Aborted Attack on Iran." *New York Times*, Sept. 21, 2019. https://www.nytimes.com/2019/09/21/us/politics/trump-iran-decision.html.

Baraniuk, Chris. 2015. “Ashley Madison: ‘Suicides’ over Website Hack.” *BBC*, August 24, 2015. http://www.bbc.com/news/technology-34044506.

Barrett, Brian. 2019. “The Air Force Will Let Hackers Try to Hijack an Orbiting Satellite.” *Wired*, September 17, 2019. https://www.wired.com/story/air-force-defcon-satellite-hacking/.

Borghard, Erica D., and Shawn Lonergan. 2017. “The Logic of Coercion in Cyberspace.” *Security Studies* 26, no. 3: 452–481. https://doi.org/10.1080/09636412.2017.1306396

Chesney, Robert. 2019. “Crossing a Cyber Rubicon? Overreactions to the IDF’s Strike on the Hamas Cyber Facility,” *Lawfare*, May 6, 2019. https://www.lawfareblog.com/crossing-cyber-rubicon-overreactions-idfs-strike-hamas-cyber-facility.

Danzig, Richard. 2014. *Surviving on a Diet of Poisoned Fruit*. Washington, D.C.: Center for a New American Security. https://s3.amazonaws.com/files.cnas.org/documents/CNAS_PoisonedFruit_Danzig.pdf.

Futter, Andrew. 2018. *Hacking the Bomb: Cyber Threats and Nuclear Weapons*. Washington, D.C.: Georgetown University Press.

Gartzke, Erik and Jon R. Lindsay. 2017. “Thermonuclear Cyberwar.” *Journal of Cybersecurity* 3, no. 1 (March): 37–48. https://doi.org/10.1093/cybsec/tyw017.

Ghafur, S., S. Kristensen, K. Honeyford, G. Martin, A. Darzi, and P. Aylin. 2019. “A Retrospective Impact Analysis of the WannaCry Cyberattack on the NHS.” *Nature*, October 2, 2019. https://www.nature.com/articles/s41746-019-0161-6.

Goodin, Dan. 2015. “First Known Hacker-Caused Power Outage Signals Troubling Escalation.” *ArsTechnica*, January 4, 2015. arstechnica.com/security/2016/1/first-known-hacker-caused-power-outage-signals-troubling-escalation/.

Goodin, Dan. 2017. “Hackers Trigger Yet Another Power Outage in Ukraine.” *ArsTechnica*, January 11, 2017. https://arstechnica.com/security/2017/01/the-new-normal-yet-another-hacker-caused-power-outage-hits-ukraine/.

Gorman, Siobhan and Julian Barnes. 2011. “Cyber Combat: Act of War.” *Wall Street Journal*, May 31, 2011. https://www.wsj.com/articles/SB10001424052702304563104576355623135782718.

Greenberg, Andy. 2018. “The Untold Story of NotPetya, the Most Devastating Cyberattack in History.” *Wired*, August 22, 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Greenberg, Andy. 2019. “New Clues Show How Russia’s Grid Hackers Aimed for Physical Destruction: A Fresh Look at the 2016 Blackout in Ukraine Suggests that the Cyberattack Behind it was Intended to Cause far More Damage.” *Wired*, September 12, 2019. https://www.wired.com/story/russia-ukraine-cyberattack-power-grid-blackout-destruction/.

Healey, Jason. 2019. “The Implications of Persistent (and Permanent) Engagement in Cyberspace.” *Journal of Cybersecurity* 5, no. 1: 1–15. https://doi.org/10.1093/cybsec/tyz008.

InfoSecurity. 2013. “Cyber-terrorism Shut Down Israel’s Carmel Tunnel.” October 28, 2013. http://www.infosecurity-magazine.com/news/cyber-terrorism-shut-down-israels-carmel-tunnel/.

Jensen, Benjamin, and Brandon Valeriano. 2019. *What Do We Know about Cyber Escalation? Observations from Simulations and Surveys*. Washington, D.C.: Atlantic Council. https://www.atlanticcouncil.org/wp-content/uploads/2019/11/What_do_we_know_about_cyber_escalation_.pdf.

Kahn, Herman. 1965. *On Escalation: Metaphors and Scenarios*. New York: Praeger.

Kostyuk, Nadiya, and Yuri M. Zhukov. 2017. "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?" *Journal of Conflict Resolution* 63, no. 2: 317–347. https://doi.org/10.1177%2F0022002717737138.

Kreps, Sarah, and Jacquelyn Schneider. 2019. "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-Based Logics." *Journal of Cybersecurity* 5, no. 1. https://doi.org/10.1093/cybsec/tyz007.

Leavitt, Lydia. 2011. "NASA Confirms Satellite Hacks in Congressional Advisory Panel." *Engadget*, November 2, 2011. https://www.engadget.com/2011/11/02/nasa-confirms-satellite-hacks-in-congressional-advisory-panel/.

Lin, Herbert. 2012. "Escalation Dynamics and Conflict Termination in Cyberspace." *Strategic Studies Quarterly* 6, no. 3 (Fall): 46–70. www.jstor.org/stable/26267261.

McElroy, Damien, and Ahmad Vahdat. 2013. "Iranian Cyber Warfare Commander Shot Dead in Suspected Assassination." *The Telegraph*, October 2, 2013. http://www.telegraph.co.uk/news/worldnews/middleeast/iran/10350285/Iranian-cyber-warfare-commander-shot-dead-in-suspected-assassination.html.

Morgan, Forrest E., Karl P. Mueller, Evans Medeiros, Kevin L. Pollpeter, and Roger Cliff. 2008. *Dangerous Thresholds: Managing Escalation in the 21st Century*. Santa Monica, CA: RAND.

Murgia, Madhumita. 2015. "Could Cyberattack on Turkey be a Russian Retaliation?" *The Telegraph*, December 18, 2015. http://www.telegraph.co.uk/technology/internet-security/12057478/Could-cyberattack-on-Turkey-be-a-Russian-retaliation.html.

Nakashima, Ellen. 2011. "U.S. Cyberweapons Had Been Considered to Disrupt Gaddafi's Air Defenses." *Washington Post*, October 17 2011. https://www.washingtonpost.com/world/national-security/us-cyber-weapons-had-been-considered-to-disrupt-gaddafis-air-defenses/2011/10/17/gIQAETpssL_story.html.

Newman, Lily Hay. 2018. "China Escalates Hacks against the US as Trade Tensions Rise." *Wired*, June 22, 2018. https://www.wired.com/story/china-hacks-against-united-states/.

Perlroth, Nicole. 2012. "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back." *New York Times*, October 23, 2012. https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html.

Reuters. 2012. "Suspected Cyber Attack Hits Iran Oil Industry." April 23, 2012. https://www.reuters.com/article/us-iran-oil-cyber/suspected-cyber-attack-hits-iran-oil-industry-idUSBRE83M0YX20120423.

Sanger, David and Mark Mazzetti. 2016. "U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict." *New York Times*, February 16, 2016. https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html.

Schneider, Jacquelyn. 2017. "Cyber and Crisis Escalation: Insights from Wargaming." https://pacs.einaudi.cornell.edu/sites/pacs/files/Schneider.Cyber%20and%20Crisis%20Escalation%20Insights%20from%20Wargaming%20Schneider%20for%20Cornell.10-12-17.pdf.

Tucker, Patrick. 2019. "The NSA Is Studying Satellite Hacking." *Defense One*, September 20, 2019. https://www.defenseone.com/technology/2019/09/nsa-studying-satellite-hacking/160009/.

Valeriano, Brandon, Benjamin Jensen, and Ryan Maness. 2008. *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford, U.K.: Oxford University Press.

United Nations. 2015. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/70/174. http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

Zetter, Kim. 2015. "The NSA Acknowledges What We All Feared: Iran Learns from US Cyberattacks." *Wired*, February 10, 2015. https://www.wired.com/2015/02/nsa-acknowledges-feared-iran-learns-us-cyberattacks/.