Working Paper

SWP Working Papers are online publications within the purview of the respective Research Division. Unlike SWP Research Papers and SWP Comments they are not reviewed by the Institute.

SWP

RESEARCH DIVISION INTERNATIONAL SECURITY | WP NR. 01, DECEMBER 2020

Cyber Escalation

The conflict dyad USA/Iran as a test case

Matthias Schulze, Josephine Kerscher, Paul Bochtler

Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

Contents

Introduction

At the beginning of July 2020, a series of detonations in the Iranian nuclear fuel enrichment plant in Natanz triggered fears of a Stuxnet 2.0.[1] The Stuxnet computer worm, which physically destroyed Iranian nuclear centrifuges in 2010, is considered by many as the starting point for the smoldering cyber conflict between Iran and the USA.[2] Stuxnet is still considered to be one of the most aggressive cyber attacks to date because it was the first digital malware to cause damage in physical space, thus reaching a new level of intensity. In the words of former NSA director Gen. Michael Hayden, "someone crossed the Rubicon" with Stuxnet.[3]

The conflict dyad USA-Iran is particularly interesting from the perspective of cyber security research and international relations since disputes are carried out in the cyber- and information space as well as in the conventional, physical domain. The interaction between the two cyber powers has a "cross-domain" dimension, which has been rarely studied so far.

Since 2018, the USA has a new cyber security policy of "persistent engagement" that some regard as potentially escalating.[4] In addition, the conflict escalated in early 2020 as a consequence of the targeted killing of Iranian General Soleimani in January. In view of the US presidential elections in 2020, many security experts expected costly and destructive cyber retaliatory strikes by Iran as the Islamic Republic is now considered a serious cyber power that does not shy away from aggressive, destructive attacks. Since Iran has shown interest in targeting critical infrastructures in the US, a potentially damaging retaliatory cyber attack cannot be ruled out completely.[5] The likelihood of a destructive cyber retaliation in response to a conventional attack is uncertain and research on escalation dynamics in cyberspace and across domains is still in its infancy.

Literature Review on Cyber Escalation

Ben Buchanan has shown in his book that cyber attacks can be conceptualized with the theoretical toolkit of international relations. In his work, he argues that cyber attacks, due to uncertainty, strategic ambiguity, and subjective interpretation can cause escalation dynamics and security-dilemmas.[6] Escalation generally means an increase in the intensity of a conflict, for example through threats or concrete, harmful actions. Escalation intensity can increase quantitatively if the same tools and techniques of statecraft are used with in-

[1] Farnaz Fassihi et al., "Iran Admits Serious Damage to Natanz Nuclear Site, Setting Back Program", in: *New York Times* (online), 5.7.2020, https://www.nytimes.com/2020/07/05/world/middleeast/iran-Natanz-nuclear-damage.html (Last accessed 20.8.2020).
[2] Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare", in: *Security Studies* 22,no. 3 (2013): 365–404.
[3] Sean Lawson, "Cyber Threat Projection and the Insider Threat: Stuxnet Edition", in: *Forbes* 2012 (Juni 2012), https://www.forbes.com/sites/seanlawson/2012/06/02/cyber-threat-projection-and-the-insider-threat-stuxnet-edition/.
[4] Jacquelyn Schneider, "Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy", 10.5.2019, https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy (Last accessed 20.8.2020).
[5] Sean Lyngaas/Shannon Vavra, "After U.S. kills Iranian general, analysts warn of Tehran's ability to retaliate in cyberspace", *Cyberscoop* 2020 (Januar 2020).
[6] Ben Buchanan, *The cybersecurity dilemma. Hacking, trust and fear between nations* (New York, NY, 2017).

creased frequency. It can also be enhanced qualitatively with a shift to other, more expensive means or policy fields.[7] For example, the expulsion of diplomats can be answered with severe economic sanctions, which will be understood as an escalating move.

This increase is commonly represented by the concept of an "escalation ladder". Escalation ladders hierarchize conflict intensities and define political actions and behavior for each level or rung of the ladder, that favor an ascent or descent of the conflict intensity. Not all activities lead to increased tensions in the form of a crisis or an open war. According to Herman Kahn, one of the founders of the concept, espionage, diplomatic gestures, and active measures of influence are described as "sub crisis maneuvering", which takes place at a low level of conflict.[8] These activities do not necessarily ignite wars. However, disruptive actions or the use of force indicate crisis move up on the escalation ladder. The level of crisis defined by high tensions is followed by the level of conventional war or armed attacks. After that come nuclear engagements, first the use of tactical nukes, and then later, at the high end of the ladder, strategic nuclear attacks against civilian populations. The latter result in existential threats to states, which is why they have a special quality.

Sarah Kreps and Jacquelyn Schneider argue, that there exists a firebreak between the conventional and nuclear levels of escalation: even if limited, conventional attacks are carried out by an aggressor, most decision-makers are deterred from escalating to the nuclear level. Most decision-makers are deterred from escalating to the nuclear level as it is being perceived as particularly dangerous in qualitative terms. Due to these firebreaks in between the escalation levels, states tend to act reciprocally: they use proportional, comparable reactions to unfriendly acts ("tit for tat") that tend to stay on the same rung of the ladder.[9]

It is unclear whether these firebreaks also exist between the cyber domain and the conventional domain. Furthermore, it is unclear how cyber escalation ladders function, and how different cyber activities correlate to different escalation levels. In 2015, the US introduced the concept of equivalence: cyber attacks can be answered with conventional attacks if they reach a certain threshold. NATO adopted this stance in 2016 whereas states like Russia, China, and Cuba contest this concept at the UN level.[10] The problem is that cyber-attacks can have diverse characteristics, levels of intrusiveness, and levels of effects. They can achieve the level of physical destruction, as Stuxnet showed, but rarely do so. Although cyber doomsday scenarios of cyber attack induced power outages are prominent in the media, the majority of activities in the cyber domain falls into the category of cyber crime, relatively harmless cyber espionage, and hacktivism.[11] Therefore, cyber scholars like Herb Lin argue, that cyber attacks should be considered as “sub crisis maneuvering” in the logic of Kahn’s escalation ladder. Since most cyber attacks are simple harassment, it

[7] Erica D. Borghard and Shawn W. Lonergan, "Cyber Operations as Imperfect Tools of Escalation", *Strategic Studies Quarterly* Fall 2019 (2019), https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-13_Issue-3/Borghard.pdf.

[8] Herman Kahn, "On Escalation", in *U.S. nuclear strategy*, ed. Freedman Bobbitt et al., (1989) 283–336, doi: 10.1007/978-1-349-19791-0_20.

[9] Sarah Kreps and Jacquelyn Schneider, "Escalation firebreaks in the cyber, conventional, and nuclear domains: moving beyond effects-based logics", *Journal of Cybersecurity* 5, no. 1 (2019): 1–11.

[10] Anders Henriksen, "The end of the road for the UN GGE process. The future regulation of cyberspace", *Journal of Cybersecurity* 5, no. 1 (2019): 425.

[11] Sean Lawson, "Beyond Cyber-Doom. Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats", *Journal of Information Technology & Politics* 10, no. 1 (2013): 86–103.

can therefore be argued that "cyber" comes on the level before armed, conventional conflicts on the escalation ladder.[12] If this is the case, cyber attacks do not inherently lead to escalation. More so, cyber attacks as a reaction to a conventional attacks can potentially deescalate a situation.

This finding has been confirmed in a series of wargaming conflict simulations with military and political decision-makers, but also in the context of surveys.[13] These studies have been conducted in the US. The participants did not perceive cyber attacks as an escalating means and used them, if at all, only as a retaliatory measure when the level of conventional attacks had already been reached. They reacted to conventional attacks with cyber attacks to defuse the situation. If there is an alternative between conventional retaliation and a cyber attack, wargaming participants were more likely to choose the latter. Cyber attacks thus represent a kind of "offramp" to avoid costly conventional escalation or to reduce the intensity of a conflict.

Against this finding, it can be argued that these attitudes can of course be country-specific. Threat perceptions and response patterns vary across countries with different levels of state power and varying strategic cultures.[14] It is not clear that states have the same idea of conflict ladders or even about the arrangements of the individual levels (cyber before or after the conventional level). In fact, states are likely to assess the potential damage of cyber and information operations differently. For example, authoritarian regimes tend to frame cyber threats more in the logic of information warfare. Thus, influence operations that discredit the ruling party can easily be perceived as existential threats. In highly technology-dependent Western states, cyber attacks against the power grid are bound to be considered as existential threats.[15] As a result, there is no consensus on which digital actions are particularly escalating and which are more conflict-reducing. How do cyber attacks against election campaigns and the manipulation of public discourse by means of digital disinformation relate to the temporary but reversible shutdown of critical infrastructures, or even to their permanent physical destruction with sabotage malware such as Stuxnet? Are these three very different cyber activities to be considered equally important? Which of these activities are considered escalating by states depends on their perceptions and strategic culture. This opens up the space for misunderstandings.

The second argument against the de-escalating properties of cyber attacks is the long-term historical trend. Cyber attacks have a long-term tendency to cross red lines. Attack types that were considered unthinkable and sacrosanct a few years ago are the norm today.[16] In the middle of the 2000s, "Distributed Denial of Service attacks" were the method of choice, which usually only resulted in reversible, temporarily disruptive effects. Nowa-

[12] Herb Lin quoted in: Max Smeets, "The Strategic Promise of Offensive Cyber Operations":*Strategic Studies Quarterly* Fall (2018): 90–113 (98).
[13] See Sarah Kreps and Debak Das, "Warring from the virtual to the real: Assessing the public's threshold for war over cyber security", *Research & Politics* 4, no. 2 (2017), 205316801771593; Benjamin Jensen and Brandon Valeriano, "What do we know about cyber escalation? Observations from simulations and surveys", 2019, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/what-do-we-know-about-cyber-escalation-observations-from-simulations-and-surveys/.
[14] See Jensen and Valeriano [see Fn. 13]; Miguel A. Gomez and Eula B. Villar, "Fear, Uncertainty, and Dread: Cognitive Heuristics and Cyber Threats", *Politics and Governance* 6, no. 2, (2018): 61.
[15] Alexander Klimburg, *The Darkening Web. The War for Cyberspace* (New York, 2017).
[16] I owe this argument to Jason Healey and Robert Jervis who presented this idea at Zoom Workshop in summer 2020.

days, new attack techniques such as ransomware, or attacks against cyber physical systems or Internet of Things devices allow a new quality of damage. For example, during the Cold War, acts of sabotage against the control infrastructure of strategic nuclear weapons were considered a red line because it would put nuclear deterrence in jeopardy.[17] Today, the manipulation of nuclear missiles is being actively considered, if not already carried out.[18] Cyber attacks are thus historically characterized by an upward spiral of the qualitative intensity of actions.

This short literature review leaves us with the following question to study: are cyber-attacks an offramp that can reduce conflict intensity in a conventional war or do they escalate even further? Since the question of whether a state uses cyber capabilities to escalate naturally depends on its security strategy and strategic culture, the next sections briefly characterizes the cyber security policy of Iran and the US. It is argued that the Iran-US conflict dyad is a useful case to study the research question.

Iran‘s Cyber Operations

Iran began building offensive cyber capabilities in response to Stuxnet in 2010, and these have improved steadily since then.[19] Iran has long been regarded as a tier three cyber power, indicating a relatively low level of technical sophistication.[20] Over the years, Iran certainly made progress and is now considered to be a tier two cyber power, being able to launch more complex and potentially destructive attacks.[21] Cyber attack capabilities are of great importance to Iran’s leadership. In the Iranian security strategy, offensive cyber capabilities serve as the fourth pillar of the so-called "deterrence complex". This includes, firstly, the asymmetric ability to disrupt shipping traffic in the Strait of Hormuz, secondly, the missile program, and thirdly, support for proxy terrorist groups in the region.[22] Cyber attacks are seen as a means of asymmetric confrontation with stronger opponents. Although such enemies cannot be defeated conventionally, they are still digitally vulnerable. Cyber attacks are intended to punish undesirable behavior of opponents or to change their cost-benefit calculation in such a way that foreign actors are deterred from engaging in a conventional conflict with Iran.[23]

It appears that Iranian elites consider cyber warfare to be more dangerous than physical confrontations.[24] This could imply that Iran has a different hierarchy of the escalation ladder. Cyber capabilities are regarded as an existential guarantee of security, which should

[17] Benjamin B. Fischer, "CANOPY WING: The U.S. War Plan That Gave the East Germans Goose Bumps", *International Journal of Intelligence and CounterIntelligence* 27, no. 3, (2014): 431–464.
[18] See Erik Gartzke and Jon R. Lindsay, "Thermonuclear cyberwar", *Journal of Cybersecurity* 27, (2017): 781.
[19] Yaakov Katz, "Iran embarks on $1b. cyber-warfare program", *The Jerusalem Post* (online), 18.12.2011, https://www.jpost.com/Defense/Iran-embarks-on-1b-cyber-warfare-program (Last accessed 20.8.2020).
[20] Barbara Slavin and Jason Healey, *Iran: How a Third Tier Cyber Power Can Still Threaten the United States*, Atlantic Council, 2013, https://www.files.ethz.ch/isn/168166/irancyber_ib_atlanticcouncil.pdf (Last accessed 20.8.2020).
[21] Barbara Slavin, "Opinion: Iran Advances Beyond 'Third Tier' Cyber Power", 9.5.2015, https://www.voanews.com/world-news/middle-east-dont-use/opinion-iran-advances-beyond-third-tier-cyber-power (Last accessed 20.8.2020).
[22] Hadi Ajili and Mahsa Rouhi, "Iran’s Military Strat", *Survival* 61, no. 6 (2019): 139–152.
[23] Gabi Siboni and Sami Kronenfeld, *Iran and Cyberspace Warfare*, 2012 (INSS Insight, Nr. 375).
[24] Gregory Rattrayet al. (Eds.), *Strategic Culture and Cyberwarfare Strategies: Four Case Studies* (SIPA Capstone Workshop), p. 99, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiQt

ensure the survival of the regime. They are also an important complement to hegemonic efforts. Cyber capabilities seem to be a perfect match for Iran's security strategy since they are cost-effective, enable a challenge to conventional superior powers, can be plausibly denied at the same time, and can be integrated into the deterrence complex. Thus, in addition to its own cyber units in the Revolutionary Guards and the intelligence services, Iran relies on proxy actors, i.e. loosely state-controlled or tolerated hacker groups/cyber criminals and patriotic hackers.[25]

Iran's cyber operations are generally considered to be very aggressive, as they explicitly aim to paralyze the economic core-infrastructure of antagonists in order to cause deliberately painful economic damage.[26] Examples of this are the "Shamoon" attacks since 2013, which were directed against Saudi Arabia's primary source of income, the oil industry. Data on over 13,000 computers of Saudi Aramco, the biggest oil producer in the world, have been permanently deleted by Shamoon.[27] If it cannot strike the US directly, Iran also uses punitive measures against allies of the USA like Israel. Allegedly, Iran is also constantly probing US critical infrastructure like power grids to achieve backdoor access for future exploitation.[28] In addition, Iran has a strong interest in economic and political cyber espionage of strategic rivals in the region but also globally (especially in the area of petrochemical industries). Iran also relies heavily on digital surveillance of dissidents at home and abroad.[29]

The first attempts have also been made with information operations. Iranian influence operations make use of methods established by Russia since 2016, such as botnets and troll armies in social media. Instead of creating confusion and polarization, Iranian information operations are aimed at spreading pro-Iranian narratives.[30] There are increasing reports that, in addition to Russian and Chinese actors, Iranian hackers are also trying to infiltrate the election campaigns of Joseph Biden and Donald Trump, potentially in an attempt to manipulate the US presidential election or to gather intelligence.[31]

7G71M7qAhVQMewKHQhcDd4QFjABegQIAxAB&url=https%3A%2F%2Fsipa.columbia.edu%2Ffile%2F7168%2Fdownload%3Ftoken%3DqLvPL-J8&usg=AOvVaw1dTurF0HlTv0RduDfLgHgF.

[25] Collin Anderson and Karim Sadjadpour, *Iran's Cyber Threat. Espionage, Sabotage and Revenge*, Carnegie Endowment for International Peace, 2018, https://carnegieendowment.org/2018/01/04/iran-s-cyber-threat-espionage-sabotage-and-revenge-pub-75134 (Last accessed 20.8.2020).

[26] Marie Baezner, *Hotspot Analysis: Iranian cyber-activities in context of regional rivalries and international tensions*, (ETH Zürich Center for Security Studies, 2019, p. 13), https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/20190507_MB_HS_IRN%20V1_rev.pdf (Last accessed 20.8.2020).

[27] Charlie Osborne, "Shamoon data-wiping malware believed to be the work of Iranian hackers", 20.12.2018, https://www.zdnet.com/article/shamoons-data-wiping-malware-believed-to-be-the-work-of-iranian-hackers/.

[28] Associated Press, "Iranian hackers infiltrated U.S. power grid, dam computers, reports say", *CBC* (online), 22.12.2015, https://www.cbc.ca/news/technology/hackers-infrastructure-1.3376342.

[29] Mehdi Khalaji, *Iran Intensifying Its Crackdown on Citizens Abroad*, The Washington Institute, 2.11.2018, https://www.washingtoninstitute.org/policy-analysis/view/iran-intensifying-its-crackdown-on-citizens-abroad (Last accessed 20.8.2020).

[30] Emerson T. Brooking and Suzanne Kianpour, *Iranian Digital Influence Efforts. Guerilla Broadcasting for the Twenty-First Century* (Washington, D.C., 2020), https://www.atlanticcouncil.org/wp-content/uploads/2020/02/IRAN-DIGITAL.pdf (Last accessed 20.8.2020).

[31] Shannon Vavra, "Google: Biden and Trump campaigns targeted by separate spearphishing campaigns", *Cyberscoop* (online), 4.6.2020, https://www.cyberscoop.com/biden-trump-china-iran-hacking-spearphishing-2020-elections/.

US Cyber Operations

The US is considered a tier one power which means it is able to carry out very complex, covert cyber attacks with 0-day malware. Since 2018, the Pentagon has been pursuing a new cyber strategy of permanent interaction, called "persistent engagement", with antagonists.[32] Instead of having to be authorized by the President as before, US Cybercommand can now independently initiate proactive cyber attacks against opponents. Iran is a declared antagonist in this strategy, hence, Iranian hackers are to be confronted permanently. The goal is to expose attack tools, share the relevant information for cyber defense and thus mitigate the disruptive potential. The strategy also includes an element of "defending forward": instead of reactively countering cyber attacks on US territory, they should be observed at the source, i.e. in Iranian and foreign networks, and neutralized as early as possible. In short, Iranian hackers should be so busy defending against US cyber activities that there is no time left for their own attacks. The hope is that this will increase the costs of cyber attacks against the USA and thus tie up limited resources for expensive cyber attacks.

At a superficial glance, persistent and continuous cyber attacks against Iranian networks seem like a road to escalation. But according to Michael Fischerkeller and Richard Harknett, the main proponents of this approach, the aim is not to escalate, but to establish a level of agreed competition without the resort to armed attacks. The strategy is designed to manage escalation insofar as antagonists, through continuous interaction, implicitly agree on a level of intensity of their actions in the long run. In other words, through persistent engagement, cyber attackers and defenders get to know each other and are better able to evaluate and interpret their respective actions. The hope is, that this will decrease the risk of misinterpretation and unwanted escalation in the long run.[33]

Since 2019, the USA has deliberately been more vocal and more offensive towards Iran by engaging in a strategy of "maximum pressure". This strategy has shown effects in 2020, as the US has been more willing to conduct announced cyber attacks.[34]

Empirical Analysis of Cyber Escalation Dynamics

To answer the question as to what extent the cyber conflict intensity between the USA and Iran is increasing or decreasing in quantity or quality, the authors have created a database of cyber attacks by the two states.[35] We collected openly available press reports in which either Iran or the USA were named both as the target and the suspected origin of the cyber attacks. Due to Iran's strategy to punish US allies, we also included attack campaigns that had multiple targets. We are aware that the attribution problem, i.e. the technical difficulty of identifying attackers with high degrees of certainty, is a problem in any quantitative analysis. This can lead to distortion effects in the data. Therefore, we operate with the term "alleged" attacker since we cannot be 100% sure if Iran or Iranian proxies are indeed responsible for some of the attacks. The lack of clarity on the subject of attribution is a

[32] Schneider [see Fn. 4].
[33] Michael Fischerkeller and Richard Harknett, "Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation", *The Cyber Defense Review* 2019, (2019): 267–287.
[34] Ariane Tabatabai and Colin P. Clarke, "Maximum Pressure Still Won't Sway Iran", 2020, https://www.lawfareblog.com/maximum-pressure-still-wont-sway-iran.
[35] See https://airtable.com/shrdtUE2YFlBzJjcc.

methodological problem in quantitative analyses of cyber incidents, which this analysis cannot avoid.

A total of 44 publicly acknowledged cyber interactions were collected over a period from early 2019 to July 2020. Cyber attacks are often classified, hence the exact date of some attacks could not be established. Further, some actors engaged in public attribution only make vague statements about the exact dates of attacks. Sometimes attacks are still ongoing after being detected. Other times, attribution reports only mention that a region was targeted over a longer period of time without giving clear start or end dates. Therefore, the time of the first press coverage was used as the relevant date for a cyber event. Whilst long-term trends can be identified through this approach, tit-for-tat escalation patterns in short periods of time cannot be measured granularly. Consequently, it remains uncertain whether some counter-reactions are intentional reactions to a previous attack if the chronological order of events is not fully clear.
These 44 incidents were then coded in their conflict intensity in a "double-blind" procedure. The authors used a simple, six-step cyber conflict ladder as developed by Kostyuk and colleagues.[36] They developed an escalation ladder with six levels or rungs to allow a comparison between conventional actions and cyber activities. This works well as a heuristic for cross-domain escalations, even if the grouping of activities on the respective levels can be criticized.

Successful attacks against critical infrastructure were coded as "Level 5: major damaging attack", while espionage operations were coded as "Level 2: minor harrassment".

[36] Nadiya Kostyuik et al., "Determinants of the Cyber Escalation Ladder", *The Cyber Defense Review* 3, no. 1 (2018): 123–134.

In sum, this heuristic allows creating a baseline of escalation levels and intensities over the course of several critical events. This allows us to assess whether the intensity and/or

Figure 1 Cyber-Escalation ladder by Kostyuk Et al. 2018

Spectrum of Conflict	Escalation Ladder	Conventional Actions	Cyber Actions
	Preparation	• Training • Infrastructure development • Implement SOPs	• Recruit, train, organize hackers • Develop plans • Cyber defense, counter espionage
	Minor Harassment	• Diplomatic protest • Legal action • Espionage	• Public influence, propaganda • Cyber espionage, cyber counterintelligence • Gathering credentials
UNSTABLE PEACE	Major Harassment	• Economic sanctions	• Overt demonstration of cyber capability • Inconveniencing attacks (DOS embassies & minor services, SWATing, tie up EFR resources)
	Minor Damaging Attacks	• Limited kinetic attacks (raids, drone strikes)	• Destruction of non-critical data • Targeted harassment of military infrastructure (DOS, logistics interference)
INSURGENCY	Major Damaging Attacks	• Limited contingency operations[25]	• Targeted military interference • Overt targeted disabling and/or destruction of military targets or infrastructure
		• Major military operations (invasion, regime change)	
GENERAL WAR	Catastrophic Attacks		• Permanent damage to civilian infrastructure (mass destruction of critical data, infrastructure control software, banking infrastructure)
		• Nuclear War	
	Existential Attack		• Nothing (yet)

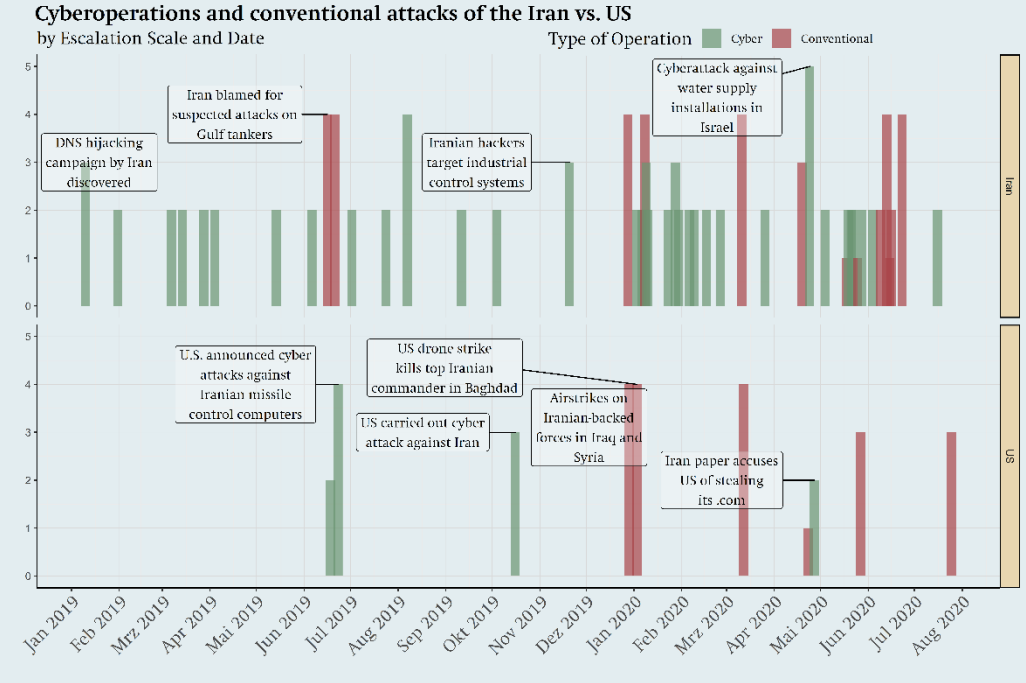
the frequency of cyber or conventional attacks is increasing. In addition to activities in the cyber domain, the authors have also collected 24 events in the conventional domain, such as missile attacks on US bases or the killing of General Soleimani in January 2020. These events span the same period and are coded according to the same methodology. This allows a comparison of the cyber domain with the conventional domain in the course of the period 2019 to mid-2020. With this sequence analysis, it can be determined whether critical, conventional events, such as the killing of Soleimani, are answered with equally critical cyber attacks (or whether deescalating measures were used).

Nevertheless, another important caveat remains in the analysis: cyber espionage attacks that are harmless in themselves can be used to prepare destructive attacks. Cyber espionage is often employed to gain a foothold on a system that can be exploited in future escalations. This means that even if a cyber espionage attack was usually coded as a "minor harassment" in the analysis, it cannot be ruled out that this shifts into a “major damaging attack” in the future. The data set does not cover this.

Findings

One central result immediately catches the eye and that is the quantity of attacks. Iran is far more visible and active in cyberspace than the USA (Figure 2).

Figure 2 Cyber and Conventional Attacks by Iran and the USA



Source: Cyber Attack Database https://airtable.com/shrdtUE2YFlBzJjcc

In the analysis period, there are 34 cyber attacks allegedly conducted by Iran (and/or its proxies), but only four by the USA. Iran tends to use lower-threshold cyber attacks in higher frequency than the USA. On average, Iranian cyber attacks are discovered every 17 days. Iran seems to follow a strategy that is supposed to cause pain through "a thousand little cuts". That Iran is using high-frequency cyber attacks to challenge the US in an asymmetric fashion is to be expected if one considers Iran's cyber strategy.

The USA uses cyber attacks far less frequently, more selectively, with stronger effects and higher intensity. Analyzing the quality dimension of the attacks, the following can be deduced. The mean value of the intensity of cyber attacks by Iran and the USA is at level 2 ("minor harassment") and at level 2.5 respectively, which is lower than the mean value of conventional attacks, which is 3.5 for Iran and 3 for the USA ("major harassment"). This seems to confirm that cyber operations are not escalating in principle, but that their intensity lags behind conventional attacks. Cyber is mostly "sub crisis maneuvering" as the intention of most attacks seems to be cyber espionage. Although Iran and the USA find themselves in a latent conflict there were only two instances in which the intensity of the conflict rose to level 5 of the "major damaging attack". This was a (thwarted) cyber attack by Iran on Israel's water supply systems.[37] Considering the climate conditions in the region, a successful disruption of drinking water in the middle of summer could have been

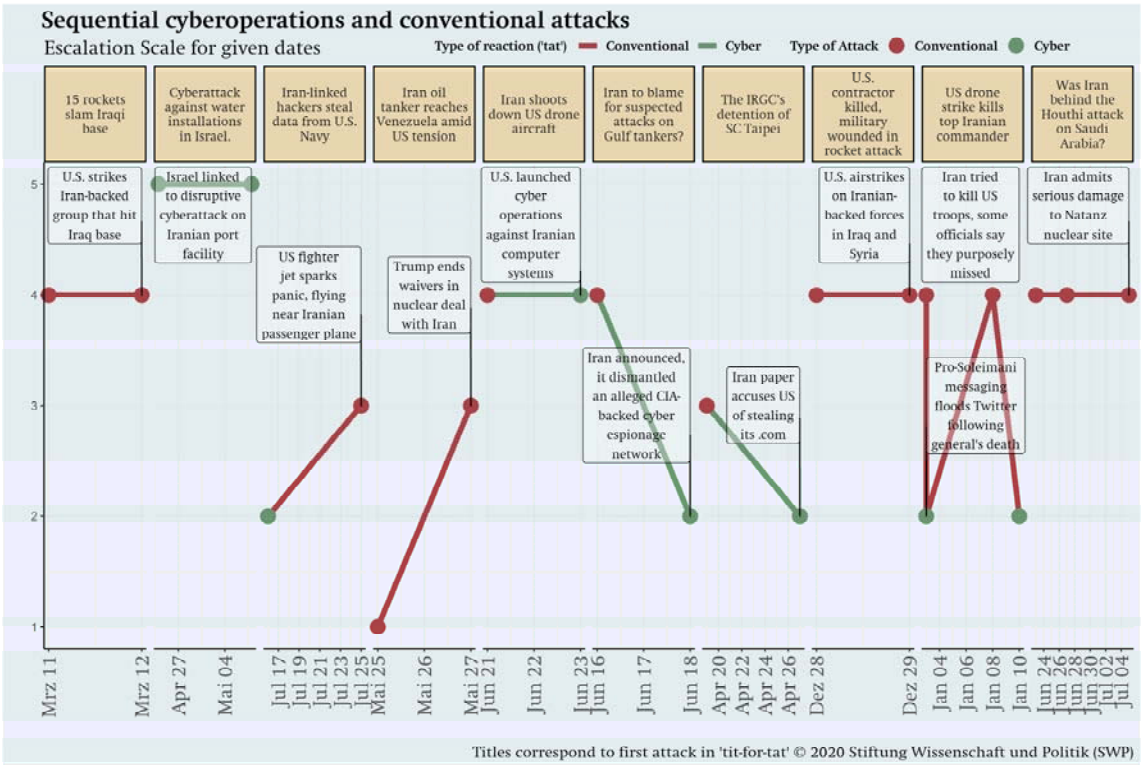
[37] Toi Staff, "Iran cyberattack on Israel's water supply could have sickened hundreds – report", *The Times of Israel* (online), 1.6.2020, https://www.timesofisrael.com/iran-cyberattack-on-israels-water-supply-could-have-sickened-hundreds-report/ (Last accessed 20.8.2020).

devastating. Israel retaliated with a similar intensity cyber attack on an Iranian port facility, resulting in some disruption of port activity.[38] The attack was included in the analysis because Israel is an important ally of the USA.

For the USA, there is some preliminary evidence in the data that seems to confirm the "offramp hypothesis". The USA uses cyber attacks as an alternative to destructive, conventional attacks. The announced cyber operations to deactivate Iranian missile systems in June 2019 stand out in this context.[39] American forces certainly could have launched a conventional attack, permanently destroying the missile system, but decided in favor of a cyber operation with prior announcement. The prior announcement is rather unusual for cyber attacks because it can diminish their effectiveness, but underlines the intended signaling effect of this action. This finding supports our hypothesis that cyber is a potentially de-escalatory alternative to conventional strikes.

However, the findings on the "offramp thesis" are not fully clear. If we look at event clusters, i.e. conventional and cyber events that take place in close temporal or "tit-for-tat" sequence, we find only two concrete events in which conventional actions ("tit") were answered with cyber attacks ("tat") of lower intensity (see Figure 3). The figure maps reaction patterns for event clusters with lots of activities in shorter periods of time and gauges the intensity of these actions.

Figure 3 Tit for Tat Event Cluster



[38] Joby Warrick and Ellen Nakashima, "Officials: Israel linked to a disruptive cyberattack on Iranian port facility", *Washington Post* (online), 18.5.2020, https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html (Last accessed 20.8.2020).

[39] Associated Press, "US launched cyber attack on Iranian rockets and missiles – reports", *The Guardian* (online), 23.6.2019, https://www.theguardian.com/world/2019/jun/23/us-launched-cyber-attack-on-iranian-rockets-and-missiles-reports (Last accessed 20.8.2020).

Source: Cyber Attack Database https://airtable.com/shrdtUE2YFlBzJjcc

We find that it is more likely that attacks are answered with reactions of similar intensity ("tit for tat"). Conventional attacks are more likely to be answered with conventional counter-reactions than with cyber attacks. If a cyber reaction to a conventional attack happens, then this usually has a similar intensity level, which also speaks for a "tit for tat" logic. If an actor wants to escalate, he/she seems to rely on conventional attacks instead of cyber attacks. From this snapshot analysis, it also appears, that a cyber attack does not automatically beget a cyber response. This seems to indicate a "Las-Vegas effect": what happens in cyber stays in cyber.

Looking deeper into the data set, the event cluster at the end of 2019 and the beginning of 2020 are quite interesting. Here the frequency of attacks is increasing and the conflict is increasingly being fought in the conventional domain. The killing of the Iranian General Soleimani and the subsequent rocket attacks on US military bases are the central events. During this event cluster, cyber attacks play a minor role whereas conventional attacks reach a higher level of intensity. This episode seems to indicate that the fears of some cyber experts have not yet materialized: Iran has so far (as far as is publicly known) not reacted with escalating, high-intensity cyber attacks on critical infrastructures in the USA, but rather has reacted conventionally with attacks on US bases. In addition, level 5 destructive cyber attacks ("major damaging attack") require a certain amount of preparation before they are ready for deployment. Since the FBI and the US Department of Homeland Security warned of increased Iranian cyber espionage activity in critical US infrastructures in the aftermath of the events, this danger still exists.

We did not, however, find evidence for a long-term intensity increase. The intensity level of cyber attacks stays relatively the same over the entire duration of the analysis. It can be argued that the spike in frequency and intensity can be accounted to the conventional component of the conflict in January 2020. Of course, the analyzed time frame covering only two years is rather short to account for long term trends. Iran launched destructive attacks like Shamoon in the past and certainly still has the capacity to repeat this in the future. We certainly require more data to make a final call about longer-term trends.

Discussion and Implications

The analysis has a few limitations. Firstly, there is little research on the question of whether Iran and the US have the same understanding of escalation ladders. Perceptions of how damaging an attack is can vary. A different, e.g. more granular coding of attack intensities, is of course conceivable and may produce a different picture of escalation intensities. One could, for example, differentiate between first or second-order effects or include damage estimates such as financial losses. This type of data is, however, not easily available.

Secondly, there is far less public information about US cyber attacks than Iranian ones. This is potentially due to the higher capability level of the USA that allows a stealthier approach, which is less likely to be discovered. Moreover, many actors working in the attribution industry tend to focus more on Iran than on Western countries, which leads to a distortion in the available data. What we know of Western cyber attacks often is the result of leaks or insider discussions, rather than research findings in the wild. However, judging

from the US persistent engagement strategy, there should be a lot of activity going on in Iranian networks. Unfortunately, by relying on public sources alone, we have little insight.
A third problem is that Iran uses proxy actors and an asymmetric retaliation strategy and escalates, for example, against US partners and other regions of the world. This makes it difficult to assess whether a cyber attack is really an intended counter-reaction to a conventional attack by the US (causality) or whether it is just an accidental reaction (correlation). In the cyber domain, we rarely have smoking-gun evidence that a cyber attack was an intended reaction to a previous attack. There are a few instances, where, for example, Iran publicly threatens retaliation to US attacks, but from this alone it is hard to judge which subsequent cyber attack is in fact carrying the retaliatory message.
Furthermore, no statements can be made on the extent to which the findings can be generalized to other cases or conflict actors.

For the time being, the thesis that cyber attacks do not escalate by themselves seems to be confirmed. Cyber attacks are usually answered with cyber counter-attacks of approximately the same intensity. This finding should be confirmed by further research because it is not clear under which conditions this applies. It is quite conceivable that states with other cyber strategies, such as North Korea or Russia, react completely different to cyber attacks. Additionally, the US-Iran conflict is also special because it already arrived at the level of conventional escalation. This makes it obvious to react to armed attacks with more conventional measures since conventional troops are already in place. It is unclear whether this finding also applies to states that are still at other levels of the conflict, or that are not in close geographic proximity.
In future research, we will expand our data-set to account for longer time frames. This should allow us to test the hypothesis if cyber attacks witness a qualitative increase in intensity or not.

Matthias Schulze is the deputy head of the security research division.

Josephine Kerscher was an intern at SWP from May to July 2020.

Paul Bochtler is a data-scientist at SWP.

The authors thank Veronika Datzer for editing.

SWP
Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

Ludwigkirchplatz 3–4
10719 Berlin
Telephone +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

doi: 10.18449/2020WP13