

Determinants of the Cyber Escalation Ladder

Nadiya Kostyuk

Scott Powell

Matt Skach

ABSTRACT

This article investigates how the speed and sophistication of cyber tools shape modern conflict. Using the United States as a case study, it looks at how, when, and why physical and cyber affronts can quickly escalate, and what appropriate counter-actions exist at each stage of the conflict. We also briefly contrast the US physical and cyber conflict escalation ladders with those of China and Russia. Our work has important implications for policy-makers and military leaders as it demonstrates the importance of having cyber escalation ladders for each country. We stress that not only should these ladders include country-specific perceptions of various actors and their likely motivations, but they should also account for other actors' differences in perception of various physical and cyber actions. The latter could lead to a difference in each state's understanding of the others' escalation ladders, and thus unexpected responses.

Keywords: *cyber escalation ladders, cyber conflict, spectrum of conflict, the US, China, Russia*

The first known cyberattack to cause an electrical power outage occurred in Ukraine at the end of 2015.^[1] On December 23rd, hackers disabled control systems used to coordinate remote substations, leaving people in Kyiv, the capital of Ukraine, and the western part of the country without power for several hours. A year later, presumably the same group of hackers attacked the power grid in Kyiv. The Security Service of Ukraine blamed the Russian government for both nefarious acts.^[2] The computer security firm *iSight Partners* attributed these hacks to Sandworm; a group believed to have Russia origins.^[3] Because of inferior cyber capabilities, the Ukrainian government decided not to retaliate but to verbally condemn the Russian government for this act of *cyber warfare*.^[4] If Sandworm, representing the Russian government, had faced a better-equipped opponent, the cyber events could have quickly escalated in virtual and, potentially, physical fronts.

© 2017 Nadiya Kostyuk, Scott Powell, Matt Skach



Nadiya Kostyuk is a Fellow for the Cybersecurity Project at the Belfer Center and is completing her PhD at the University of Michigan in Political Science and Public Policy. She is also a research fellow at the Cybersecurity, Internet Governance, Digital Economy, and Civic Tech Initiative at Columbia's School of International and Public Affairs during the 2017-2018 academic year. Nadiya's research interests are states' cyber capacities; cyberattacks as coercive tools; mapping physical and 'digital' fronts. Her regional expertise includes post-Soviet countries. She is currently a fellow at EastWest Institute of Global Cooperation in Cyberspace Initiative.

Spectrum of Conflict

We use the Spectrum of Conflict (“the Spectrum”, thereafter) as defined in the 2008 Army Field Manual 3-0, Operations^[5] (“The Manual”, thereafter), to outline the Spectrum of Conflict for conventional and cyber actions. The manual divides the Spectrum of conflict into stable peace, unstable peace, insurgency, and general war.^[6] At each stage, the US, its allies, and its adversaries—state or non-state actors—have various cyber tools available. Additionally, motivations for these actions vary as widely as the tools and types of actors that employ them.^[7] Having determined potential suspects of cyberattacks and their possible motive, an actor should decide where to place the committed cyber misbehavior in the Spectrum, as well as where the other side similarly perceives such action on their Spectrum.^[8] For instance, a hostile actor may conduct espionage during stable peace, but could also conduct the same activity during insurgency or unstable peace. Depending on these perceptions, state and non-state actor responses may vary.

Escalation Ladder

When deciding the appropriate response to a cyberattack, the US should account for the following factors. *First, who is the attacker, and what is their objective?* For instance, industrial espionage may not require a declaration of war, but sabotage of the power grid may require more than a denial of service attack. *Second, where does the US consider itself in the Spectrum?* If it is in unstable peace, diplomatic actions or brandishing capabilities may prove to be useful deterrents. When conducting an exercise to brandish capabilities, the US should determine if exposing a capability is useful and what end-state is it trying to achieve—making an adversary look powerless or the US to appear powerful.^[9] Finally, *second-order effects are worth*



Scott Powell is a former Army officer and 2005 graduate of the United States Military Academy. He is also a recent graduate of the Gerald R. Ford School of Public Policy.

considering; these effects can include unintended damage, whether physical or otherwise, and the possibility of further escalation by an adversary.

In this section, we build a cyber escalation ladder (Table 1) aligning the Spectrum of Conflict, a proposed escalation ladder, and the types of kinetic (non-cyber) and cyberattacks that may emerge at each level.

Building the Ladder

The Spectrum of Conflict's lowest rung is a stable peace. In this preparatory phase, cyber activity is directed towards developing the capability to offensive and defensive cyber actions. This means that effective cyber forces, even with no immediate threat on the horizon, must continuously build and maintain its cyber capabilities by recruiting, training and organizing cyber forces as well as providing them with the financial, technological, organizational, and infrastructure resources needed for their mission. In addition, these forces should develop contingency plans and be ready to defend against threats in cyberspace that appear with little or no advanced warning. These conditions are needed in preparation for an adversary taking hostile actions towards unstable peace or any other form of escalation.

In a conflict that escalates into minor harassment, cyber activities expand to exploit weaknesses in an adversary's system without disrupting operations or damage infrastructure. The mission of the US cyber forces at this Spectrum level incorporates all of the prior actions and expands to include espionage and cyber counterintelligence, gathering credentials, and propaganda. Credential collection is an important activity to launch larger scale cyberattacks or facilitate the access of information on protected systems.^[10] As intelligence gathering is an accepted norm, it should not be considered escalatory.



Matt Skach is a PhD candidate in the Department of Computer Science and Engineering at the University of Michigan, and a combat engineer in the 1433rd Engineering Company of the Michigan Army National Guard. His research interests include novel design and technologies for large-scale computer systems and data centers. Skach has an MS in electrical engineering from the University of Michigan and a BS in electrical engineering from Oregon State University.

Propaganda, although not explicitly a cyber-attack, can incorporate cyber elements to enhance the spread or impact of a message. In response to the early conflict in Ukraine, social media emerged as a major channel of communication for protesters and international observers, and Russia utilized the “comments” section of news sites to promote pro-Russian dialogue on domestic and foreign websites.^[11] In a more direct approach that may cross the border into unstable peace occurred during the 2016 US Presidential Election. Russia combined an extensive propaganda campaign with cyber-attacks on the Democratic National Committee and subsequent release of damaging emails through WikiLeaks in an attempt to influence the outcome.^[12]

Moving upwards from stable peace to an unstable peace, cyber activities at the major harassment level aggressively exploit weaknesses and disrupt daily operations, but do not cause permanent damage to infrastructure or compromise systems. On the conventional (non-cyber) side, sanctions are a common tool used by the US and exemplified by their reaction to Russian interference in the 2016 Presidential election.^[13] At this stage, equivalent cyber operations include overt demonstrations of cyber capability to deter the opponent and minor denial of service (DOS) attacks that exert influence but do little permanent damage. Overt displays of cyber capability such as the defacement of public websites were a common tool of the hacktivist group Anonymous during Operation China in response to China’s crackdown on protests.^[13] Similarly, DOS attacks that deny cyber or non-cyber infrastructure can pose varying levels of inconvenience against an adversary. Lizard Squad, a hacktivist group, launched distributed denial of service (DDOS) attacks against Sony’s PlayStation Network and Microsoft’s Xbox Live services.^[15] Website defacement

and DDOS by an adversary can present a significant inconvenience but poses little risk of permanent damage.

Although initiated in cyberspace, the impact of DOS and DDOS attacks are not limited to the cyber domain. ‘SWATing’^[16] and other attacks that focus on emergency services, if applied on a large scale, could be used to tie up law enforcement resources and other emergency first responders (EFR). SWATing style attacks pose an increased risk of injury or loss of life over DOS cyberattacks, but neither of these incursions alone is likely to be escalatory.

Moving up the escalation ladder from harassment to minor damaging attacks, cyberspace enables a range of low-financial-cost attacks that compromise non-critical data or inflict minor, repairable damage. Potential targets include the destruction of non-critical data on networked systems and the targeted harassment of military infrastructure. Sony Pictures suffered a massive data loss in 2014 at the hands of North Korean state hackers,^[17] and Saudi Aramco lost data on 35,000 hard drives in a 2012 cyberattack.^[18] The attacks did not pose a significant disruption of services outside of the affected company, and neither event prompted retaliation, but both companies faced severe financial costs to restore services. On the other hand, WannaCrypt,^[19] one of the most significant Ransomware attacks to date, demonstrated the compelling capability to tie up businesses and critical services such as hospitals by encrypting data and holding it ransom until demands are met. There exists the potential for extensive collateral damage from this type of cyberattack. This is fundamentally different from traditional DOS attacks that temporarily make a site or service inaccessible, as opposed to Ransomware that may permanently destroy data if demands are not met.

Although WannaCrypt primarily struck unpatched civilian targets, there is the potential for targeted harassment of military infrastructure. Interference actions that target non-critical military services stand to interrupt day-to-day operations by delaying email communication or hindering logistics, but do not pose a significant threat to critical military infrastructures such as strategic missile or air defense systems. Similarly, interference or delay of supplies can pose a problem, but outside of a war zone, it is unlikely to pose a critical threat to combat readiness. Highly targeted attacks with limited destructive capability such as Stuxnet^[20] may also be deployed at this level. These attacks are not inherently escalatory, but depending on the target and duration of the attack the risk posed by the vulnerability may be considered escalatory (e.g., hindering communications may be seen as the prelude to a larger attack). Smaller cyberattacks may also become escalatory when paired with other kinetic attacks. A DOS attack on EFR services combined with a limited kinetic action such as a drone strike could increase the net effect from a minor damaging attack to a major one when EFR resources are not immediately available to treat casualties.

Continuing to escalate from minor to major damaging attacks, where conventional kinetic attacks come into play, cyberattacks escalate to include compromising critical data and causing damage to systems or infrastructure that is not quickly repaired and degrades military capabilities. Both kinetic and cyberattacks at this level are designed to disable or destroy critical military infrastructure; disabling early warning systems, as well as targeted instruction or information dispersal. In an early example of cyber warfare, the Israeli military subverted and disabled Syrian air defenses before conducting an aerial strike on a Syrian nuclear facility.^[21] The US military also proposed but ultimately decided against an attempt to disable Iraqi air defenses through a cyberattack before the 2003 invasion.^[22] The US did, however, email instructions to Iraqi military officers using Iraq's email system on how they should surrender to Coalition forces before the ground invasion.^[23] These and larger cyberattacks should be considered escalatory in nature.

Beyond major damaging attacks lie catastrophic and existential attacks. A catastrophic cyberattack is one that compromises national security and requires a response so massive it would prevent the US from addressing other contingencies for the duration of the conflict. Existential attacks are those that would potentially result in the destruction of the US or collapse of its society, for example, a bilateral nuclear war.

Permanent damage to civilian infrastructure such as power and utility grids has the potential to become a catastrophic attack affecting millions of people. At present, we do not believe a single mode of cyberattack alone would pose an existential threat to the US, however, this may change in the near future. Although many (if not most) utility grids are currently connected to the Internet, they are segregated regionally by hundreds of local companies that reduce the potential impact of a widespread outage. However, in addition to critical utility grids, food production and logistics are rapidly becoming automated and connected to the Internet.^[24] A large-scale, long-lasting attack on the food production or supply distribution network once manual systems are sufficiently scarce could create devastating casualties comparable to a small-scale nuclear strike.

The Ladder

In Table 1, we assemble the Spectrum of Conflict and associated actions at each level into a single ladder. The first column contains the Spectrum of Conflict, from Stable Peace to General War, and the second column includes levels of damage from No Activity up through Catastrophic Attacks. Column 3 lists potential actions and responses using non-cyber options, and column 4 provides examples of cyberattacks that align with the options from column 3. As some rungs of the ladder or types of attacks may occur in more than one category, the boxes from one column may overlap boxes from another column to indicate the different levels of possible actions and consequences.

Spectrum of Conflict	Escalation Ladder	Conventional Actions	Cyber Actions
	Preparation	<ul style="list-style-type: none"> Training Infrastructure development Implement SOPs 	<ul style="list-style-type: none"> Recruit, train, organize hackers Develop plans Cyber defense, counter espionage
	Minor Harassment	<ul style="list-style-type: none"> Diplomatic protest Legal action Espionage 	<ul style="list-style-type: none"> Public influence, propaganda Cyber espionage, cyber counterintelligence Gathering credentials
UNSTABLE PEACE	Major Harassment	<ul style="list-style-type: none"> Economic sanctions 	<ul style="list-style-type: none"> Overt demonstration of cyber capability Inconveniencing attacks (DOS embassies & minor services, SWATing, tie up EFR resources)
	Minor Damaging Attacks	<ul style="list-style-type: none"> Limited kinetic attacks (raids, drone strikes) 	<ul style="list-style-type: none"> Destruction of non-critical data Targeted harassment of military infrastructure (DOS, logistics interference)
INSURGENCY	Major Damaging Attacks	<ul style="list-style-type: none"> Limited contingency operations²⁵ 	<ul style="list-style-type: none"> Targeted military interference Overt targeted disabling and/or destruction of military targets or infrastructure
		<ul style="list-style-type: none"> Major military operations (invasion, regime change) 	
GENERAL WAR	Catastrophic Attacks	<ul style="list-style-type: none"> Nuclear War 	<ul style="list-style-type: none"> Permanent damage to civilian infrastructure (mass destruction of critical data, infrastructure control software, banking infrastructure)
	Existential Attack		<ul style="list-style-type: none"> Nothing (yet)

Table 1: Escalation Ladder


Differences in Perceptions Leading to Potential Escalation

Potential adversaries such as Russia and China have similar views on the escalation ladder when it comes to the online environment, but some important differences do exist. Besides the most commonly used cyber tools, such as espionage,^[26] DDOS and spear-phishing, both countries give a high priority to their information space. Harmony in society is vital for China and Russia, and inciting anti-government propaganda, for instance, might be considered an existential threat.

China's Internet is subject to the control of the Ministry of Public Security.^[27] Also, the government uses computer specialists for managing its domestic blogosphere.^[28] The government tries to create an impression of freedom of speech by planting people in online debates to influence public opinion.^[29] One goal of the state is to shield its Internet users from outside influences—mainly from Western countries—aiming to block such issues such as “human rights, democracy, and religion.”^[30] Besides being protected by the Great Firewall, the Chinese People's Liberation Army (PLA) remain alert in case such a threat from the West arises.

Such concern is widely shared by Russia, whose greatest fear is “circulation of [uncontrolled and Western-influenced] information.”^[31] Western cybersecurity experts believe Russia is afraid that its entire population could serve as the target of influence for an enemy disinformation campaign.^[32] This concern is even documented in the country's laws^[33] that outline the circumstances in which Russia would deploy its armed forces in the territory of other states to provide information security.^[34] Even a minor violation of such harmony in the society supported by the control of information can quickly lead to escalation on the cyber action ladder. Creating Russia's and China's escalation ladders is a crucial step for future research on this topic.

CONCLUSION

By 2020, on average, each American will have five internet-connected devices that bring various vulnerabilities that are readily exploitable during a conflict. States should be aware of each other's position on physical and escalation ladders before engaging in a cyber conflict. Using the US as a case study, we demonstrated the challenges that nation-states face when forming appropriate responses to US cyber actions. These challenges also apply to other state actors. Not only should they decide who the attackers are and their likely motivations, but they should account for other actors' differences in perception of various actions. The latter could lead to a difference in each state's understanding of the other's escalation ladder, and unexpected responses. Therefore, it is important to understand what norms each state associates with various attacks, and what it may infer about the attacker's intentions since “in cyberspace as in other realms of warfare, ‘the defender frequently does not understand how threatening his behavior, though defensively motivated, may seem to the other side.’”^[35] 

Acknowledgements

We would like to thank the CDR reviewers and editors for their helpful comments and feedback. We would also like to thank Professor Robert Axelrod of the Gerald R. Ford School of Public Policy at the University of Michigan for his guidance and input. Company and product names within this publication are used for identification purposes and may be trademarks of their respective owners.

NOTES

1. Ellen Nakashima, “Russian hackers suspected in attack that blacked out parts of Ukraine,” *The Washington Post*, January 5, 2016.
2. Kim Zetter, “Everything we know about Ukraine’s power plant hack,” *Wired*, January 20, 2016.
3. *Ibid*.
4. Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017).
5. Even though FM 3-0 is now ADP/ADRP 3-0 with an update in 2016, we decided to use the older version of the document FM 3-0, as the new one does not have a spectrum of conflict in it. Despite the fact that we are using the older version, our main argument does not change.
6. Department of the Army, “FM 3-0 C-1”, February 2008. This manual defines *stable peace* as “an operational environment characterized by the absence of militarily significant violence.” The manual defines *unstable peace* as the conditions “when one or more parties threaten or use violence to accomplish their objectives, stable peace degenerates into *unstable peace*. Unstable peace may also result when violence levels decrease after violent conflict.” The manual defines *insurgency* as “the organized movement of subversion and violence by a group or movement that seeks to overthrow or force change of a governing authority.” The manual defines *general war* as the conditions when “armed conflict between major powers in which the belligerents have used all their resources, and the national survival of a major belligerent is in jeopardy. Diplomatic and economic channels have broken down.”
7. Some potential motivations may include money, espionage, skills for employment, fame, entertainment, hacktivism, terrorism, or war. From: Jason Andress and Steve Winterfeld, *Cyber warfare: techniques, tactics and tools for security practitioners* (Elsevier, 2013), 48.
8. Differences in perception will be discussed in the later section.
9. Martin C. Libicki, *Brandishing Cyberattack Capabilities* (Rand Corporation, 2013), vii-xi.
10. Kim Zetter, “NSA Hacker Chief Explains How to Keep Him Out of Your System,” *Wired*, January 20, 2016.
11. Shaun Walker, “Salutin’ Putin: inside a Russian troll house,” *The Guardian*, April 2, 2015; David Stern, “The Twitter War: Social Media’s Role in Ukraine Unrest,” *National Geographic*, May 11, 2014.
12. “U.S. Intelligence Report Identifies Russians Who Gave DNC Emails to Wikileaks,” *Time*, January 5, 2017.
13. David Sanger, “Obama Strikes Back at Russia for Election Hacking,” *The New York Times*, December 29, 2016.
14. Mary-Ann Russon, “Anonymous brings down 30 Chinese government websites to support Hong Kong protestors,” *International Business Times*, April 13, 2015.
15. Dylan Love, “Why Microsoft and Sony couldn’t stop Lizard Squad attack despite warnings,” *International Business Times*, December 30, 2014.
16. Federal Bureau of Investigation, “The Crime of ‘Swatting,’” September 12, 2013.
17. Peter Elkind, “Sony hack,” *Fortune Magazine*, July 1, 2015.
18. Jose Pagliery, “The inside story of the biggest hack in history,” *CNN*, August 5, 2015.
19. David Sanger, Sewell Chan and Mark Scott, “Ransomware’s Aftershocks Feared as U.S. Warns of Complexity,” *The New York Times*, May 14, 2017.
20. Kim Zetter, “How digital detectives deciphered STUXNET, the most menacing malware in history,” *Wired*, August 11, 2011.
21. Richard Alan Clarke and Robert K. Knake, *Cyber War* (Harper-Collins, 2010), 1-9.
22. *Ibid*.
23. *Ibid*, 9-11.
24. Dave Bradford, “Old McDonald had an algorithm-driven prescriptive planting service,” *Cyber Risk Network*, November 4, 2012; George Westerman, “The Internet-connected engine will change trucking,” *Harvard Business Review*, November 4, 2012.

NOTES

25. For definitions see: Pub, Joint, “3-0. Doctrine for Joint Operations,” *Washington DC: Joint Chiefs of Staff* (1995).

26. For instance, China is famous for its cyber espionage operations (Reveron 2012); The Mandiant report highlights the peculiarities of the Chinese hacking U.S. infrastructure, government, ministries, and financial sector for over a decade with the main purpose of stealing information (Westby 2013); Derek S. Reveron, *Cyberspace and national security: threats, opportunities, and power in a virtual world* (Georgetown University Press, 2012); Jody Westby, “Mandiant report on Chinese hackers is not news but its approach is.” *Forbes Magazine*, February 20, 2013.

27. Derek S. Reveron, *Cyberspace and national security: threats, opportunities, and power in a virtual world* (Georgetown University Press, 2012).

28. *Ibid*

29. *Ibid*

30. Nigel Inkster, “China in cyberspace,” *Survival* 52, no. 4 (2010), 55-66.

31. Kerstin Pertermann, *Challenges in cybersecurity: risks, strategies, and confidence-building; international conference* (Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg, 2012).

32. “Conceptual Views on the Activity of the Russian Federation Armed Forces in Information Space,” Section 1, Fundamental Terms and Definitions, *The Russian Federation* (NATO Cooperative Cyber Defense Centre of Excellence, 2011); Timothy L. Thomas, *Recasting the Red Star: Russia Forges Tradition and Technology through Toughness* (Foreign Military Studies Office, 2011).

33. These laws include: the 2000 Doctrine of the Information Security of the Russian Federation (RF) and the 2011 “Conceptual Views on the Activity of the Russian Federation Armed Forces in Information Space.”

34. Keir Giles, “Russia’s public stance on cyberspace issues,” (IEEE: Cyber Conflict (CYCON), 2012 4th International Conference, 2012), 1-13.

35. Barry R. Posen, “Inadvertent Nuclear War? Escalation and NATO’s Northern Flank,” *International Security* 7, no. 2 (1982), 28-54.