Military Cyber Affairs

Volume 3 | Issue 2 Article 6

December 2018

Systemic Cyber Risks and Defense: Valuation, Innovation and Strategic Implications

Pythagoras N. Petratos
Blavatnik School of Government, Oxford University, p.pythagoras@yahoo.com

Systemic Cyber Risks and Defense: Valuation, Innovation and Strategic Implications[1]

Pythagoras N. Petratos[2]

The Economic Undertheorizing of Systemic Cyber Risks

A broad consensus exists among experts that cyberattacks are increasing both in number, variety, and sophistication. Some cyberattacks such as phishing and attacks on critical infrastructures are aimed at the whole of society and whole states, while others target specific parts of cyberspace, such as companies and military facilities. The internet has produced vast wealth and distributed knowledge in a globally free, open and borderless space. However, the economic benefits of cyberspace are continuously threatened by the rise of large scale, catastrophic, systemic cyber events. Such adverse cyber events could cause enormous disruptions to numerous systems all over cyberspace. Some of these systems might not be able to recover.

Systemic cyber risks have been relatively undertheorized despite their importance. Despite their importance, there is very limited, if any, economic analysis of systemic cyber risks. To highlight the critical importance of systemic cyber risks, let us consider how financial transactions are performed in digital systems. Financial systemic risks conversely, have been significantly theorized and researched. A significant systemic cyber disruption of digital financial systems could have the effects of a major financial crisis. In addition, a systemic cyber adverse event could have existential consequences. There could be systemic cyberattacks on military installations, detonating nuclear weapons that would escalate conflict and initiate war. Systemic cyber events can constitute casus belli, due to their substantial impact. 'Insurance against war by preparation for it is, of all methods, the most business-like' (Luce, 1891). Understanding, analyzing and

[1] Please cite as: Petratos, Pythagoras N., "Systemic Cyber Risks and Defense: Valuation, Innovation and Strategic Implications," in Demchak, Chris C. and Benjamin Schechter, eds. Military Cyber Affairs: Systemic Cyber Defense 3, no. 2 (2018).

[2] Blavatnik School of Government, Oxford University

researching systemic cyber risks and systemically defending against them can be the best way to prevent costly outcomes, conflict and ultimately the possibility of war.

Therefore, our purpose is to better understand systemic cyber risks. This paper attempts to address some conceptual flaws of cyberspace regarding the critical role of systemic cyber risks. It focuses on the impact and in particular *the valuation of the effects of potential systemic cyber risks.* Valuation is an essential and established element in theorizing the aspects of economics and constructing a broader framework for the assessment of risks. This paper briefly draws analogies from the financial sector and crises and applies them to cyber risk. It also discusses the limitations to valuation methodology that externalities, property rights and liability can bring. To make the analysis more applicable, we examine the value of IP cyber theft, innovation models and how systemic cyber risks can affect the persistence of innovation and its dominance. Finally, we discuss the strategic implications of systemic cyber risks for the private sector, the military, national power and alliances.

Systemic Cyber Risks and Financial Analogies

"*Systemic cyber risk* is the risk that a cyber event (attack(s) or other adverse event(s)) at an individual component of a critical infrastructure ecosystem will cause significant delay, denial, breakdown, disruption or loss, such that services are impacted not only in the originating component but consequences also cascade into related (logically and/or geographically) ecosystem components, resulting in significant adverse effects to public health or safety, economic security or national security." (WEF, 2016)

In general, there does not seem to be a consensus on a common definition of systemic cyber risks. Sommer and Brown (2011) find that the definition varies between the two extremes of occasions of multiple attacks on insignificant computer systems, and rather rare events that have been subject to criminal convictions.

Furthermore, there are other and major limitations to the set of existing definitions. Firstly, it is necessary to define the limits of a system. Is the focus global or regional and national? Is one referring to the whole of cyberspace or national cyber systems or Critical Information Infrastructures (CII)? Therefore, the *definition of the system* upon which the concept of systemic cyber risk is based is crucial. Usually the term 'systemic' refers to *large scale*, *catastrophic* events.

https://digitalcommons.usf.edu/mca/vol3/iss2/6
DOI: https://doi.org/10.5038/2378-0789.3.2.1060

Systemic cyber risks that could have an overall catastrophic outcome should therefore be characterized using a definable *whole system approach* combined with calculable *aggregations of risk*s.

Systemic cyber risks feature some characteristics that can assist in better defining and understanding them. (Mallery and Petratos, 2018). *Cascading* is a fundamental characteristic. However, it is essential to not only assume cascade but also to analyze its effects. What initiates a cascade and the *transmission* and *amplification channels and mechanisms*? It could be said that cascades propagate due to *complex and critical interdependencies*. The system architecture and the structure and nature of interdependencies among cyber assets define how cascades evolve and impact systems. Interdependencies highlight the *massive complexity of modern cyber systems*. (Mallery and Petratos, 2018). As the number of connected devices and related applications grows exponentially, complexity and interdependencies increase respectively. Another characteristic strongly related to complexity is the *high degree of uncertainty*. The compellingly *dynamic* character of the internet contributes to the uncertainty (Mallery and Petratos, 2018). The number of interconnected devices, applications and technological innovations rapidly change cyberspace and increase the uncertainty. Within this changing ecosystem it is difficult to observe the factors that can trigger a systemic failure and its transmission and amplification mechanisms. (Pederson et al . 2006)

An additional methodological difficulty directly related to uncertainty is that there is hardly any *historical systemic cyber precedence and data*. It is unlikely that there have been yet any systemic cyber adverse events with cataclysmic dimensions. However, there have been cyberattacks with systemic characteristics, that have cost millions and in some cases billions of dollars, As the sophistication of cyberattackers increase, it is likely to have more systemic cyber events. It remains subjective and debatable which events can be classified as cyber systemic. Nevertheless, a helpful method is to use relevant historical, economic, and other useful metaphors to enrich the discourse and provide insight into cyber strategy and policy (Goldberg and Arquilla, 2014). The *analogies with financial and economic literature* are valuable for three main reasons. Firstly, the financial and economic literature on systemic financial risks and crises has been significantly developed, particularly after the latest financial crises and bears parallelisms to cyberspace (Petratos, 2018). Secondly, the methodology of analogies between financial and cyber has been successfully used before and applied to the sub-prime crisis and the Lehman Brothers

event (Zurich, 2014). Finally, it shares similar systemic characteristics and evaluates the outcomes of adverse systemic events.

Impact Valuation, Externalities, Property Rights and Liability

It is crucial to be able to value the economic impact of cyberattacks and especially evaluate the value at risk from systemic cyber risks because this is an illustrative way to display the damage that cyberattacks can cause Simple cyberattacks do not have significant impact and it is relatively easy to value them. However, it is hard to provide an accurate valuation of large scale and systemic cyber risks. This is due to the characteristics of systemic cyber risks. The complexity of IT systems and operations, the complex and critical interdependencies involved in the propagation of cyberattacks, and the high level of uncertainty all limit successful valuation. The lack of sufficient historical data regarding systemic cyber risks is probably the biggest problem. Although there are some related data points, forecasting the level of potential damage is difficult and ambiguous.

In addition to the characteristics of systemic cyber risks, there are numerous externalities that make it even harder to value their potential impact. An IMF paper argues that 'Cyber risk is a textbook example of a systemic risk' (Kopp et al. 2017). Indeed, many characteristics of systemic risks are analogous to cyber risks, especially large scale cyber risks. These market failures include information asymmetries, strategic complementarities, coordination failure, and externalities as well as economies of scale, barriers to entry, and concentration of risk (Kopp et al. 2017). This is a wide range of market failures. Even more externalities, such as herding, contractual and other types of network externalities can be added to the list of systemic cyber risks. (Mallery and Petratos, 2018; Petratos).

An enormous drawback to evaluating the value at risk from systemic cyber threats is that property rights in cyberspace are not well defined. The ownership of information and the infrastructure in which it is transmitted is often unclear. Anonymity remains an unresolved issue. It is hard to identify the owners and distributors of information. The case of Facebook and Cambridge Analytica illustrate this problem. Identity and attribution cannot be effective without well-defined property rights. Furthermore, the problems continue with *responsibility and liability*. It is not possible to construct a theory of liability in cyberspace without property rights. *Accordingly, legal implementation and criminal conviction are ineffective, as are remedies* and

https://digitalcommons.usf.edu/mca/vol3/iss2/6
DOI: https://doi.org/10.5038/2378-0789.3.2.1060

compensation. Finally, without *well defined property rights*, *it is difficult to correct externalities* (Coase, 1960).

More attention should be paid to improving the definition of property rights in cyberspace. It is fundamental to the better valuation and assessment of risks. Without valuation one cannot effectively prioritize and invest in systemic defense, share risks, create alliances, and in general guide cyber defense policies according to the significance of the risk. "In contrast to many other financial and operational risks, loss data on cyber events is either not available or not useable for pricing cyber risk." (Kopp et al. 2017). The availability of data and disclosure of cyberattack information is not the only impediment, the methods and tools used to value (price) cyber risk also pose a problem. However, financial analogies and their application to cyberspace can prove very useful for generating systemic cyber scenarios. Systemic cyber scenarios are necessary to understand the nature and level of threats and associated risks.

IP Cyber Theft and Innovation Dominance

Our discussion so far has been theoretical. It would be useful to underline it with a practical example of systemic cyber risks and valuation by addressing innovation models commonly discussed in financial analogies. *A example that can be considered to share characteristics with systemic cyber risks is Intellectual Property (IP) theft*. Cyber IP theft incidents usually denote large scale operations and impact. It is also a persistent threat. Some figures indicate that IP theft can reach $ 600 billion per year[3]. However, this might be an underestimation or overestimation of the real figure. There is a need for better valuation models and methods (i.e. Work Factor Analysis, Mallery, 2016) to provide more accurate calculations.

There are numerous innovation models that can be challenged by cyber IP theft (i.e. production at lower cost, quicker release of products etc.). However, we would like to focus on *radical and disruptive innovation*s. Both radical and disruptive innovations are on the cutting edge of innovation. They are not concerned with imitative innovation activities, which generates much

[3] The range of estimates was from $ 255 billion to $ 600 billion annually. 'Further, while cyber espionage may have decreased from some actors, several sources report that the worst and most capable actors still persist in hacking for economic gain'. In The Commission on the Theft of American Intellectual Property by The National Bureau of Asian Research (2017). Update to the IP Commission. The Theft of American Intellectual Property: Reassessment of the Challenges and US Policy. The National Bureau of Asian Research.

lower value. In that sense disruptive and radical innovation can be deemed responsible for producing companies with extraordinary value (i.e. Amazon, Alphabet, Facebook, etc.). Moreover, these innovations can create new markets, disrupt, completely change and eventually make existing markets irrelevant[4].[5] In that sense, cyber IP theft that targets disruptive and radical innovations can be a 'game changer' in many fields. Cyber theft of high value innovations can undermine the competitive and strategic advantage of nations and change the balance of power.

Such innovations can, not only, affect markets, whole industries, national industrial structure and innovation policy, but they can also have remarkably systemic strategic and defense implications. A notable example is stealth technology and its implications for the Research and Development (R&D) process behind defense acquisitions and strategies found in modern nations. In order to develop stealth technology and the fifth generation of combat aircraft (i.e. F-35), there is a need for significant investment. The F-35 multirole aircraft can be considered a disruptive innovation, since it can render the earliest fourth generation fighters obsolete. The value of stealth technology, and in particular the F-35, is hard to estimate. It is not only the investment in this technology that defines its valuation, but a broader array of value elements, ranging from intangible assets (i.e. related IP and diffusion of technology) to the strategic value of having unique weaponry in strategies of deterrence, containment and air superiority. There are significant indications that such technology has been obtained by other nations using cyber espionage operations[6]. Similar cases can be true for naval and ground forces military innovations and technologies.

In that sense, cyber IP theft does not only have severe economic implications for wealth and employment, it can also have severe effects on the systemic innovation of states. It can furthermore have security consequences that can threaten U.S. military supremacy and superiority on multiple levels. Cyber activities and more specifically systemic cyber IP theft can challenge military and national power dominance, specifically of the United States (Nye, 2010). Iit is

[4] For a description of Disruptive Innovations see for example, Christensen et al., (2015).
[5] For a description of Radical Innovations see for example, Tellis et al., (2009).
[6] Jeff Daniels, ''Chinese theft of sensitive US military technology is still a 'huge problem,' says defense analyst'' *CNBC*, Nov 8, 2017, https://www.cnbc.com/2017/11/08/chinese-theft-of-sensitive-us-military-technology-still-huge-problem.html

https://digitalcommons.usf.edu/mca/vol3/iss2/6
DOI: https://doi.org/10.5038/2378-0789.3.2.1060

essential to design appropriate cybersecurity policies. To do the latter, it is necessary improve valuation methods for systemic and in general cyber security risks.

Conclusions and Strategic Implications

Cyber risks have numerous strategic implications. Systemic cyber risks, and especially the example of systemic cyber IP theft, by definition, can have massive economic, technology and innovation implications and bring changes to markets, industries, society and national power. We have already discussed the economic implications and innovation dominance. A useful parallelism lies between systemic cyber risks and the systemic theories and levels of analysis in international relations. The value at risk and the potential impact of systemic cyber risks can significantly affect the broader basic concepts in international relations. State sovereignty can be noticeably breached by systemic cyberattacks.

National power, soft and hard, can be also significantly affected. This is particularly true for smaller states, where systemic cyber events could substantially degrade their capabilities and consequently increase the level of threats. In the long term, cyber IP theft and other potential systemic cyber risks can change the balance of power between states. States can close economic and defense capability gaps and sometimes leapfrog. Therefore, in a complex world, and possibly related to other adverse events, cyber systemic risks could trigger frictions, cause conflict escalation and in some cases might constitute casus belli. Finally, it raises concerns about alliances and what a systemic cyberattack in a member state might mean and what reactions it would cause.

Systemic cyber risks require systemic responses and therefore a whole system approach. The first step is to define them and better understand their characteristics and the value of their potential impact. The estimation of the value at risk is crucial for appropriate prioritization, investment and cooperation. Cooperation and the formation of alliances are usually based on desired outcomes and thus the valuation of these outcomes is essential. Externalities can cause significant limitations and property rights could assist in correcting them and improving liability and legal implementation. Property rights are necessary for tackling cyber IP theft and most importantly for defining legal actions, remedies and compensation that can prevent it. At the same time, property rights are crucial for outlining national sovereignty. Norms can facilitate property rights and assist in the avoidance of systemic cyber risks. Norms and legal rules have a systemic

character (Kratochwil, 1989) and can correspond to the systemic cyber risks challenges. Norms should apply to both economic issues as well as national security dimensions.

https://digitalcommons.usf.edu/mca/vol3/iss2/6
DOI: https://doi.org/10.5038/2378-0789.3.2.1060

References

Christensen, Clayton M., Michael E. Raynor, and Rory McDonald. ‘’What Is Disruptive Innovation?’’ *Harvard Business Review*, (December 2015): 44-53.

Coase, Ronald. "The Problem of Social Cost". *Journal of Law and Economics*. 3 (1), (1960): 1–44, https:// doi:10.1086/466560

Daniels, Jeff. ‘’Chinese theft of sensitive US military technology is still a 'huge problem,' says defense analyst’’ *CNBC*, Nov 8, 2017, https://www.cnbc.com/2017/11/08/chinese-theft-of-sensitive-us-military-technology-still-huge-problem.html

Goldman, Emily O. and John Arquilla. *Cyber Analogies.* Monterey, CA: Department of Defense Analysis Naval Postgraduate School ,2014.

Kopp, Emmanuel, Lincoln Kaffenberger, and Christopher Wilson. ‘’Cyber Risk, Market Failures, and Financial Stability’’. *IMF Working Paper*, WP/17/185 (2017): 1-35.

Kratochwil, Friedrich. Rules, Norms and Decisions: On the Conditions of Practical and Legal Reasoning in International Relations and Domestic Affairs. Cambridge: Cambridge University Press,1989

Luce, Stephen B. ‘’The Benefits of War’’, *The North American Review*, Vol. 153, No. 421 (Dec., 1891): 672-683.

Mallery, John C. *An Epistemic Architecture for Measurable Security*, invited talk, Computer Science Department, University of Oxford, October 6, 2016

Mallery, John C. and Pythagoras N. Petratos. *Definitions and Characteristics of Systemic Cyber Risks*. MIT Working Paper, 2018 (forthcoming)

Nye Joseph S. Jr. ‘’The Future of American Power: Dominance and Decline in Perspective.’’ *Foreign Affairs,* Vol. 89, No. 6, The World Ahead (November/December 2010): 2-12.

Pederson, Perry, et al. ‘’Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research’’ Idaho National Laboratory Idaho Falls, Idaho 83415, 2016.

Petratos, Pythagoras N. ‘’Analogies between Financial and Cyber Stability.’’ In Stability in Cyberspace: Normative Considerations edited by Eneken Tikk, Asser Press, 2018 *(Forthcoming)*

Sommer, Peter and Ian Brown. *Systemic Cybersecurity Risk*. OECD/IFP Project on “Future Global Shocks”. Paris: OECD, 2011

Tellis, Gerard J., Jaideep C. Prabhu and Rajesh K. Chandy (2009). ‘’Radical Innovation Across Nations: The Preeminence of Corporate Culture.’’ *Journal of Marketing*, Vol. 73, No. 1, (January 2009): 3-23.

The Commission on the Theft of American Intellectual Property by The National Bureau of Asian Research. *Update to the IP Commission*. The Theft of American Intellectual Property: Reassessment of the Challenges and US Policy. The National Bureau of Asian Research, 2017

World Economic Forum, *Understanding Systemic Cyber Risk. White Paper*. Global Agenda Council on Risk & Resilience. World Economic Forum, 2016

Zurich Insurance Company. *Beyond data breaches: global interconnections of cyber risk*. Zurich Insurance Company Ltd and Atlantic Council of the United States, 2014

https://digitalcommons.usf.edu/mca/vol3/iss2/6
DOI: https://doi.org/10.5038/2378-0789.3.2.1060