Economics of Cybersecurity: Part I

By: Natalia Khaniejo
Edited by: Amber Sinha

Introduction

The twenty first century has witnessed an unprecedented conflation of everyday experiences and technosocial practices. The emergence of technologies like the Internet of Things, Cloud Computing, Digital Payment infrastructures are all emblematic of this conflation of technology with economic, social and political modes of existence. Politics and economics are increasingly being amalgamated with Cybernetic frameworks and consequently Critical infrastructure has become intrinsically dependent on Information and Communication Technology (ICTs). The rapid evolution of technological platforms has been accompanied by a concomitant rise in the vulnerabilities that accompany them. Recurrent issues include concerns like network externalities, misaligned incentives and information asymmetries. Malignant actors use these vulnerabilities to breach secure systems, access and sell data, and essentially destabilize cyber and network infrastructures. Additionally, given the relative nascence of the realm, establishing regulatory policies without limiting innovation in the space becomes an additional challenge as well. The lack of uniform understanding regarding the definition and scope of what can be defined as Cybersecurity also serves as a barrier preventing the implementation of clear guidelines. Furthermore, the contrast between what is convenient and what is 'sanitary' in terms of best practices for cyber infrastructures is also a constant tussle with recommendations often being neglected in favor of efficiency. In order to demystify the security space itself and ascertain methods of effective policy implementation, it is essential to take stock of current initiatives being proposed for the development and implementation of cybersecurity best practices, and examine their adequacy in a rapidly evolving technological environment. This literature review attempts to document the various approaches that are being adopted by different stakeholders towards incentivizing cybersecurity and the economic challenges of implementing the same.

Understanding cybersecurity

The term Cybersecurity is a complex goliath with amorphous boundaries. Determining what constitutes Cybercrime, Cybersecurity, Cyberdeterrence has been a constant challenge at the level of the state as well as the individual. With the increased intermingling of socio-economic models and Cybernetic architecture, understanding the extent of how security manifests on digital platforms and affects information is the first step to securing it. Determining the ways in which Cybersecurity differs from Physical Security[1] has also been a challenge for theorists with varying researchers applying different paradigms to Cyberspace. As stated by Ian Brown and Pete Somer in Reducing Systemic Cybersecurity Risk "[A]mong the various writers and producers of statistics, notions of what amounts to an incident, an attack , even cyberwar, vary considerably."[2] The lack of clarity regarding what gets incorporated under the umbrella term of Cybersecurity hinders the implementation of clear security frameworks. Broadly speaking, the term Cybersecurity or Information Security refers to "the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access."[3] As a discipline it emerged from concepts of computer security but it has evolved to encompass and subsume several other themes within it. In the current age, Cybersecurity broadly encompasses – Network Security, Application Security, Endpoint Security, Data Security, Identity Management, Infrastructure Security, Mobile Security, Cloud Security, Response and recovery, and End User Management. All these aspects together form a holistic picture of the various parts involved in developing a healthier cyber ecosystem for individuals, companies and governments. The increasing costs of both the infrastructure as well as the resources needed to defend it must be taken into account before developing policy initiatives aimed at securing the space. Some theorists attribute the rise in Cybercrime to insecure and unprotected IoT devices in interconnected networks. Other popular reasons that have made cybercrime more lucrative are:

1) The emergence of new attack technologies
2) Weaker cybersecurity in countries with relatively nascent access to technology
3) Increased proliferation of technology creating an increase in the number of potential victims
4) The emergence of cybercrime-as-a-service and other business schemes

[1] The term physical security is used here as territorial/national security.
[2] Brown, I., & Sommer, P. (2011). Reducing Systemic Cybersecurity Risk. OECD.
[3] Times, E. (n.d.). Definition of Cybersecurity. Retrieved from Economic Times: https://economictimes.indiatimes.com/definition/cyber-security.

5) Easier monetization of exploits.[4]

Defining deterrence and ensuring the protection of information infrastructure without necessarily constructing a non-permeable firewall in an increasingly globalized space has been a key challenge. Furthermore, there are also more layered complexities with the idea of how cybercrimes can be investigated. 'Cybercrimes' in terms of breaches and theft require very limited resources to initiate and often lead to extremely high rewards. An example of this can be seen in the 2016 sentencing of three engineers who "created an unprecedented botnet—powered by unsecured internet-of-things devices like security cameras and wireless routers—that unleashed sweeping attacks on key internet services around the globe in 2015."[5] Cybersecurity as it currently standards is lacking both in terms of prevention as well as recovery measures. In the event of a CII breach, determining culpability and attributing blame would require investigative methods that might breach another network/institution/government's jurisdiction/security practices. Determining efficient and collaborative protocol for varying levels of crime and security is inescapable in a data driven age. Methods of investigation and incentive based information sharing need to re-evaluated, to take into account the multiple sources of information that currently exist as well as the reliability of the sources themselves. "Crime, espionage and international conflict are very different threats, and grouping them together can lead to poorly framed solutions" Cybercrime can occur at various stakeholder and infrastructural levels and it is essential to understand the economic and policy incentives motivating the securitization of the environment at each level.

Cybersecurity and Economics

One of the biggest concerns while dealing with security in Cyberspace is determining the extent of what is encompassed within the realm of Cybersecurity. Given their predominant spread, ICTs have come to form a "critical nervous system of the economy, government and private life"[6] in most advanced and advancing countries today. The emergence of new forms of 'networked interaction' has led to a shift in the value associated with information, data and economics. While analysing concepts like cybercrime and cyber attack certain key conceptions to keep in mind are cost, risk, reward and recovery. The 'cost' of an attack as well as the 'cost' of defence are determined by the risk and reward of

[4] Gross, G. (2018, 02 23). The Cost of Cybercrime. Retrieved from Internet Society: https://www.internetsociety.org/blog/2018/02/the-cost-of-cybercrime/.
[5] Graff, G. M. (2017, 12 13). How a Dorm Room Minecraft Scam Brought Down the Internet. Retrieved from Wired: https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/.
[6] Bauer, J. M., & Eeten, M. V. (2011). Introduction to the Economics of Cybersecurity. Communications & Strategies, 13-21.

undertaking such an attack. For an attacker, the risk would include an analysis of the difficulty of attack combined with the probability of getting caught pitted against the reward of a successful attack and the improbability of disclosure. For a defender, the cost of defence would be determined on the basis of the probability of being targeted, calculated in conjunction with the difficulty of breaching secure systems. As stated by Joseph Cordes "[i]n principle, well-designed policies should balance benefits from defensive measures against their costs (which include important concerns about privacy)."[7] Defining these costs and statistics accurately and determining structured paths of investment that don't necessarily devolve in 'over-securitization' has proved to be a challenge in the recent years.
Accenture released a study in 2017 based on eight years of research where they state that "successful breaches per company each year has risen more than 27 percent".[8] Furthermore, the report also states that most security measures being undertaken are inefficient at best. The report states that Five of the nine security technologies had a negative value gap where the percentage spending level is higher than the relative value to the business."[9] There is a lack of investment in innovative methods of security enhancement, as well as diversified threat prevention.

The intersection of technology and economics

The conflation of economics and cybernetic technologies has taken place on multiple levels and the paradigms continue to evolve and shift with the development of newer technologies. This amalgamation of cybernetic infrastructure and economic processes can be seen in:
1) Data and information as tools of economic exchange: Knowledge is power, and in an information age, even raw knowledge – in the form of sheer data – quadruples in value. Increased globalization and digital interconnectivity has led to the emergence of transnational models of economic exchange. Data regarding usage patterns, if accrued, assimilated, distributed and analyzed would compromise individual user privacy tremendously. The lack of incentives encouraging the establishment of individual and community best practices towards cyber hygiene have culminated in an overexposure of consumer data and a breach of individual rights and privacy. Access to such information is rarely governed and the recent General Data Protection Regulation as enforced on 25th May 2018 is one of the first comprehensive efforts towards regulating data flows. The reasons why data and information have become such marketable goods is that in a capitalist economy, insight into individual customer preferences could lead to a spectrum of invasive practices ranging from tailored advertising to

[7] Cordes, J. J. (2011). An Overview of the Economics of Cybersecurity and Cybersecurity Policy. CSPRI.
[8] Ponemon Institute, A. (2017). Cost of Cybercrime. Ponemon Institute.
[9] *Ibid*.

political misinformation/manipulation. The recent US election witnessed repeated data breaches of voter information, and the manipulation of statistics as evinced by 'fake news' websites has exposed the dangers of the internet becoming a feedback loop reinforcing non reflexive users' confirmation bias. Further, data breaches have economic consequences as well. Most data breaches include information that is very closely linked to digital payment structures and the unauthorized access of information is what escalates towards financial breaches/theft. The profitable nature of information theft is reinforced by the fact that this data can then be sold on the deep web and used for malicious purposes. Examples of high level data breaches are the Equifax breach,[10] the Republican National Committee breach,[11] Uber[12] etc.

2) Private and social incentives for Cybersecurity:

The last few years have also witnessed the rise of involvement of the private sector in cybersecurity aimed at encouraging and improving holistic infrastructural hygiene. However, while an increase in private sector investments in cybersecurity would certainly go a long way in improving the security environment, leaving these efforts solely to the latter, is an unsustainable practice. Driven by profit motives, firms will often invest just enough to secure their own infrastructure. Furthermore, there is a lack of incentive for investment when private enterprises are not held liable for security mishaps. Firms would primarily be invested in preventing breaches of their infrastructure and would need added incentives to invest in long term network securitization strategies. This is where theorists like Bruce Kobayashi believe that governments could step in and remedy any perceived 'underinvestment in cybersecurity.' In *Private versus Social Incentives in Cybersecurity: Law and Economics*, Kobayashi talks about the public good nature of investing in systematic cybersecurity expenditures versus the limited but direct nature of undertaking private cybersecurity expenditures and reiterates the need for the former. Public-Private partnerships would be extremely helpful in ensuring that cybersecurity investment does not err on the side of either over or under investment.

---

[10] One of the biggest breaches of 2017, Equifax was targeted and the data of 146 million people was exposed. Weinberger, M. (2018, May). The Equifax security breach affected millions more people than we originally thought. Retrieved from Business Insider: https://www.businessinsider.in/The-Equifax-security-breach-affected-millions-more-people-than-we-originally-thought/articleshow/64083715.cms.

[11] Misconfigured database with the personal information of over 198 million voters was left unconfigured. Sullivan, D. O. (2018, May). The RNC Files: Inside the Largest US Voter Data Leak. Retrieved from Upguard: https://www.upguard.com/breaches/the-rnc-files.

[12] An example of the dangers of delayed breach notifications, Uber paid off the 20 year old hacker who hacked into its database and the company has constantly been in the line of fire due to the lack of user privacy, illegal surveillance and other such practices. McKay, T. (2017, December). Uber Settles Lawsuit Alleging It Obtained Rape Victim in India's Confidential Medical Records. Retrieved from Gizmodo: https://gizmodo.com/uber-settles-lawsuit-alleging-it-obtained-rape-victim-i-1821156541.

3) The growth of e-commerce, Financial Technologies and the rise of global payment infrastructures: The advent of the internet brought along with it not just reconfigured modes of communication but also restructured versions of market economics. The almost all pervasive presence of transnational e-commerce platforms, digitized payment systems, and more recently cryptocurrencies have forced providers as well as consumers to reorient themselves in a rapidly evolving market. As early as 2011, companies like McKinsey released studies regarding the 'world-wide' economic impact where Internet networks were presumed to have added at least 3-4 percentage points to the gross GDP of a country.[13] Currently, according to a 2016 evaluation, growth in the cybersecurity market is projected to reach $9 trillion in economic value by 2020.[14] The increased interdependence of economic and cybernetworks – as can be seen in the emergence of FinTech companies, cryptocurrencies and digital payment infrastructures – has been a key incentive motivating research around the economics of Cybersecurity. The digital payments infrastructure has changed the way traditional economic processes have been undertaken over the years and it has become essential to imagine new ways of implementing and encouraging security within the space.

"The influence of ICTs on society goes far beyond establishing basic information infrastructure. The availability of ICTs is a foundation for development in the creation, availability and use of network-based services."[15] Furthermore, questions such as who is being securitized against what, change the methods and steps to be adopted while securing infrastructure. The rise of interconnected networks has further complicated the issue by bringing together multiple nodes without necessarily securing each individual access point. In *Cybersecurity: Of Heterogeneity and Autarky*, Randal C. Picker draws attention to these changing trends while stating that networked PCs have changed the risk calculus altogether. "E-mail and the Web make the spread of viruses and bots easy, plus the hacker can initiate access to the infected machine at will."[16] Securing interconnected infrastructure, therefore, becomes a challenge due to the varying ways in which individual users can affect the network. The lack of awareness regarding Cybersecurity best practices poses a constant vulnerability within the network as most users are unaware of the risks 'Zombie Computers' pose to the entire infrastructure. In order to counter this culture of information asymmetry and non-compliance, the ITU launched a Global Cybersecurity Agenda in 2007. "The Global Cybersecurity Agenda has seven main strategic goals, built on five work

[13] Cordes, J. J. (2011). An Overview of the Economics of Cybersecurity and Cybersecurity Policy. CSPRI.
[14] Kelly, D. (2017). The Economics of Cybersecurity. 12th International Conference on Cyber Warfare and Security 2017 Proceedings. Ohio: Academic Conferences and Publishing Limited.
[15] Gercke, D. M. (2012). Understanding cybercrime: Phenomena, challenges and legal response. ITU.
[16] Picker, R. C. (2006). Cybersecurity: Of Heterogeneity and Autarky. In M. Grady, & F. Parisi, The Law and Economics of Cybersecurity. New York: Cambridge University Press.

areas: 1) Legal measures; 2) Technical and procedural measures; 3) Organizational structures; 4) Capacity building; and 5) International cooperation."[17]

[17] Gercke, D. M. (2012). Understanding cybercrime: Phenomena, challenges and legal response. ITU.