DEFENCE RESOURCES

ECONOMIC DIMENSION OF CYBERSPACE AS NEW SECURITY THREAT

BRNO

2020

Contents

LEARNING OUTPUTS

Students will know:

- Basic concepts from area of cyberspace and cyber conflict
- Basic typology of cybernetic conflict

Students will be able to:

- Demarcate all acceptable economic principles usefulness for economic analysis of cyberspace
- Explain basic algorithm of cyber conflict impacts calculation

Students will capable of:

- discussion potential costs range imposed by cyber attack

THE ECONOMIC DIMENSION OF CYBERSPACE AS NEW SECURITY THREAT

KEY TERMS

Cyberspace, cyber conflict, costs and benetits of cybersecurity, cybersecurity, cyber defence

INTRODUCTION

Threat of Cyber conflict is totally up-to-date and vital topic (Cyberspace is number one topic all important political, economic and security discussion).
Cyber-attack protection becomes government, non-profit and for-profit firms care.
Cyber-attack can lead to massive financial losses, economic instabilities or even if as a last resort to war.

Danger of Cyber conflict is now a major arena of political, economic, and military contest.

Despite this potential for harm, little agreement exists on how to respond.
One problem is the lack of understanding, especially among policymakers, about how interconnected and vulnerable our increasingly sophisticated computer networks are.
Beyond this lies a whole host of thorny analytical questions:

- What is our ability to track the source of attacks?
- How susceptible are we to "false flag" attacks where the attackers deliberately seek to "frame" another actor as carrying out an attack?
- What responsibility should governments bear for attacks carried out by their nationals on foreign governments or entities?
- How should the responsibility for defending against cyber-attacks be apportioned between government and the private sector, between national governments and the international community?
- Can deterrence work in cyberspace?

1 BASIC CONCEPTS

1.1Cyberspace

"Cyberspace is the electronic world created by interconnected networks of information technology and the information on those networks. [...] Cyber attacks include the unintentional or unauthorized access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information. The severity of the cyber attack determines the appropriate level of response and/or mitigation measures: i.e., cyber security."[162]

The novel 5th space of warfare after land, sea, air, and space, is all of the computer networks in the world and everything they connect and control via cable, fiber-optics or wireless. It is not just the Internet – the open network of networks. From any network on the Internet, one should be able to communicate with any computer connected to any of the Internet's networks. Thus, cyberspace includes the Internet *plus* lots of other networks of computers,10 including those that are not supposed to be accessible from the Internet.

Cyberspace – basic characteristic

- cyberspace is that *it cannot exist without being able to exploit the naturally existing EMS*.
- *cyberspace requires man-made objects to exist*, which again makes cyber-space unique when compared to the land, sea, air, and space domain.
- *cyberspace can be constantly replicated*
- *the cost of entry into cyberspace is relatively cheap*.
- *the offense rather than the defense is dominant in cyberspace*, for a number of reasons:
    - defences of IT systems and networks rely on vulnerable protocols and open architectures, and the prevailing defense philosophy emphasizes threat detection, not elimination of the vulnerabilities
    - attacks in cyberspace occur at great speed, putting defences under great pressure, as an attacker has to be successful only once, whereas the defender has to be successful all the time.
    - range is no longer an issue in cyberspace since attacks can occur from anywhere in the world.
    - modern society's overwhelming reliance on cyberspace is providing any attacker *a target-rich environment*, resulting in great strain on the defender to successfully defend the domain.

1.2 Cyber security risks

Cyber security risks are risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems.

1.3 Cyber Conflict

Cyber Conflict is the use of computer power for intelligence gathering or to attack the computer, communication, transportation, and energy networks of states or non-governmental groups.

1.4 Cyber Warfare

Cyber warfare refers to a massively coordinated digital assault on a government by another, or by large groups of citizens.

- It is the action by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption.
- The term cyber warfare may also be used to describe attacks between corporations, from terrorist organizations, or simply attacks by individuals called hackers, who are perceived as being warlike in their intent.

1.5 Cyber Attack

Cyber-attack is usage concrete forms of electronical means for not only intelligence activity but mainly for assault, infiltration of destruction of computer, communication, transport or power producing network privately or publicly owned.

1.6 Cyber War

Cyberwar is conflict that occurs in cyberspace among state actors and represents sort of war, based on destruction enemy by computer systems.

Impact of this form of war can take form of tangible and intangible damage from inaccessible websites to material destruction of military and civilian systems, facilities and infrastructures.

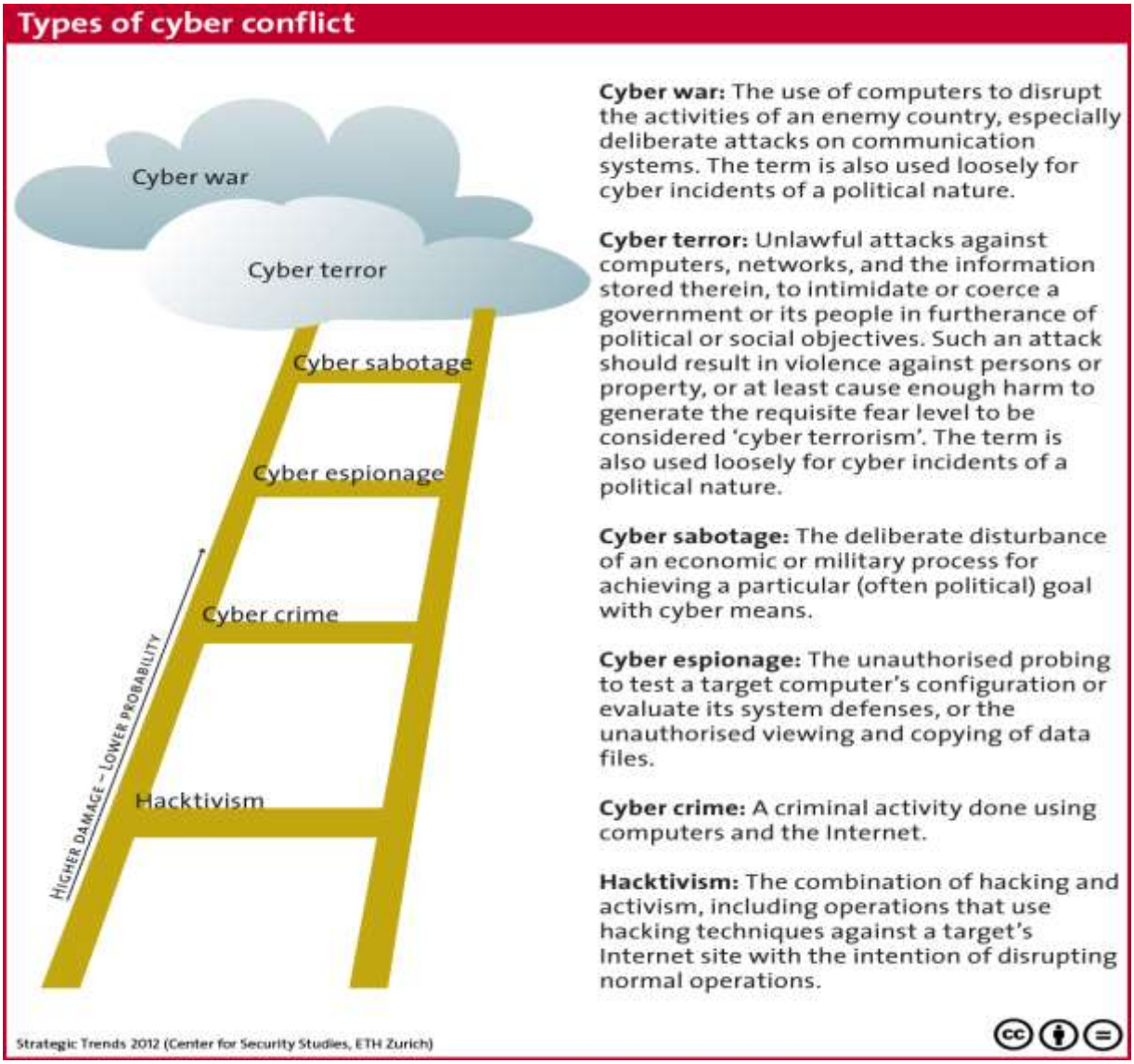
1.7 NetWar

Netwar refers to an emerging mode of conflict (and crime) at societal levels, short of traditional military warfare, in which the protagonists use network forms of organization and related doctrines, strategies, and technologies attuned to the information age.

These protagonists are likely to consist of dispersed organizations, small groups, and individuals who communicate, coordinate, and conduct their campaigns in an internetted manner, often without a precise central command.

Thus, netwar differs from modes of conflict and crime in which the protagonists prefer to develop formal, stand-alone, hierarchical organizations, doctrines, and strategies as in past efforts, for example, to build centralized movements along Leninist lines.

1.8 Cyber Conflict Classifications



2 CYBERSPACE AS A NEW SECURITY THREAT

2.1 Cyberspace as a Security Threat for national defense (Armed Forces)

For the top brass, computer technology is both a blessing and a curse. Bombs are guided by GPS satellites; drones are piloted remotely from across the world; fighter planes and warships are now huge data-processing centres; even the ordinary foot-soldier is being wired up. Yet growing connectivity over an insecure internet multiplies the avenues for e-attack; and growing dependence on computers increases the harm they can cause.

And given that computer chips and software are produced globally, could a foreign power infect high-tech military equipment with computer bugs? “It scares me to death,” says one senior military source. “The destructive potential is so great.”

2.2 Cyberspace as a Security Threat for whole society (countrywide context)

What will cyberwar look like? In a new book Richard Clarke, a former White House staffer in charge of counter-terrorism and cyber-security, envisages a catastrophic breakdown within 15 minutes. Computer bugs bring down military e-mail systems; oil refineries and pipelines explode; air-traffic-control systems collapse; freight and metro trains derail; financial data are scrambled; the electrical grid goes down in the eastern United States; orbiting satellites spin out of control. Society soon breaks down as food becomes scarce and money runs out. Worst of all, the identity of the attacker may remain a mystery.

3 ECONOMIC ANALYSIS OF CYBERSPACE

3.1 Levels of economic aspect research of cyberspace as security threat

LEVELS OF ECONOMIC ASPECTS OF CYBERSPACE RESEARCH	
Order	**Aim of research**
Level 1	Cyber conflict and war as an alternative of conventional warfare
	Cyber conflict and war as an part of conventional warfare
Level 2	Microeconomic analysis of return rate of investment and non-investment expenditures on cyber security securing
	Microeconomic analysis of optimal level of investment on cyber security and defense
Level 3	Microeconomic analysis of costs imposes on society and individuals by cyber war and cyber conflict

3.2 Economic principles usefulness for economic analysis of cybernetic security

3.2.1 Principle of the marginal opportunity costs,

3.2.2. Principle of expected marginal costs and benefits,

3.2.3 Principle of substitution,

3.2.4 Principle of diminishing returns,

3.2.5 Principle of diminishing benefits.

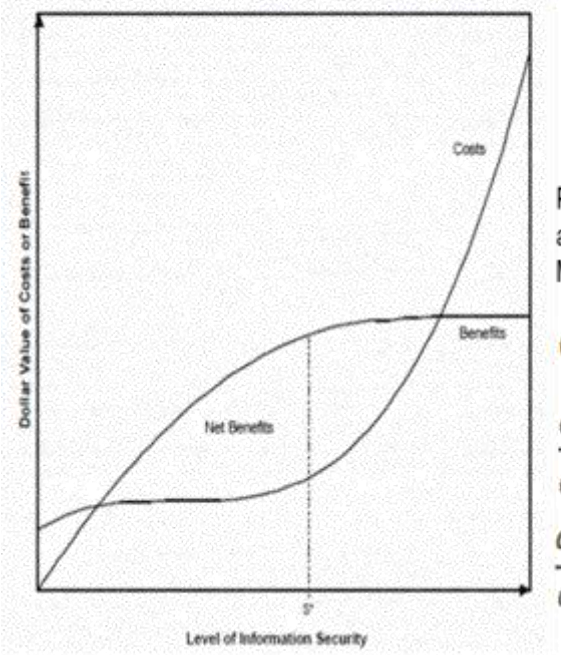
FOR BETTER UNDRSTANDING PROBLEM

More deeper insight into problem of basic economic principles usage within military robotics you can reach by study following study materials:

VAN TUYLL, Hubert., BRAUER, Jurgen. Colonizing Military History: A Millennial View on the Economics of War. Accessible on: http://www.stonegardeneconomics.com/pubs/2003_vanTuyll_Brauer_DPE_v14n3.pdf

3.3 Microeconomic analysis of cyber security securing

Microeconomic Analysis of Cyber Security providing



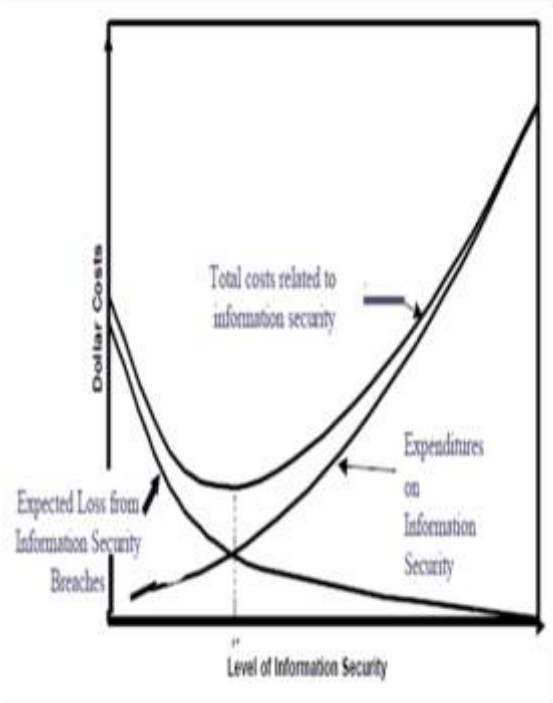
Point S* is place maximum difference between costs and benefits of securing of cyber security .
Mathematically is situation described as:

$$G(S) = B(S) - C(S)$$

$$\frac{dG}{dS} = \frac{dB}{dS} - \frac{dC}{dS} = 0$$

$$\frac{dB}{dS} = \frac{dC}{dS}$$

Microeconomic Analysis of Cyber Security providing



Total costs of cyber security providing. These costs is possible to describe following formula:

$$TC_{CS} = E_{CS} + EL_{CA}$$

where
TC_{CS} ..... total costs of cyber security providing,
E_{CS} ..... Costs of cyber security providing borne by separate endangered actors,
EL_{CA} ..... Expected impacts of cyber attack (loss of profit or damage imposed on individuals of societal organizations).

3.4 Macroeconomic analysis of cyber security securing

Macroeconomic Analysis of Cyber Security providing

$$GDP = C + I + G + NX$$

C ..... Expenditure households on consumption

I ..... Private gross homeland investment

G ..... Government Expenditure on purchase of products and services

NX ..... Net export

4 ECONOMIC ASPECTS OF POTENTIAL CYBER CONFLICT

4.1 Incentives to not Reveal Information about damages cause by cyber attack

4.1.1 Financial market impacts

The stock and credit markets and bond rating firms may react to security breach announcements. Negative reactions raise the cost of capital to reporting firms. Even firms that are privately held, and not active in public securities markets, may be adversely affected if banks and other lenders judge them to be more risky than previously thought.

4.1.2 Reputation or confidence effects

Negative publicity may damage a reporting firm's reputation or brand, or cause customers to lose confidence. These effects may give commercial rivals a competitive advantage.

4.1.3 Litigation concerns

If an organization reports a security breach, investors, customers, or other stakeholders may use the courts to seek recovery of damages. If the organization has been open in the past about previous incidents, plaintiffs may allege a pattern of negligence.

4.1.4 Liability concerns

Officials of a firm or organization may face sanctions under federal laws such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Gramm-Leach-Bliley Act of 1999 (GLBA), or the Sarbanes-Oxley Act of 2003, which require institutions to meet various standards for safeguarding customer and patient records.

4.1.5 Signal to attackers

A public announcement may alert hackers that an organization's cyber-defenses are weak, and inspire further attacks.

4.1.6 Job security

IT personnel may fear for their jobs after an incident and seek to conceal the breach from senior management.

4.2 Classification of cost imposes by cyber conflict

4.2.1.Classification of cyber conflict costs according to its character and impact

Kind of costs		**Description of costs category**
Financial costs	Civil	Loss from economic life disruption
		Loss from economic and financial infrastructure disruption
	Security (military)	Destruction of technology and weapon systems
		Damage of communication and energy infrastructure
Non-financial	Civil	Loss of reputation
		Loss of co-operation (Economic, political and alliance)
		Loss of morale of own people (soldiers, policeman, civil servants etc.)
	Security (military)	Loss of reputation (goodwill)
		Loss of co-operation interests (military co-operation and alliance)
		Loss of morale of own people (soldiers, policeman, civil servants etc.)

Resource: Own

4.2.2 Classification of cyber conflict costs according to ownership character of damaged subject

Kind of costs		**Description of costs category**
Private	**Individuals**	Loss of private information Damage of computers Withdraw finances from accounts
	Firms	Loss of business information Damage of company computers and nets Loss of company know-how (intellectual property) Outflow of customers, drain of capital (loss of business partners) Loss of financial means
Public	**State**	Disruption of critical infrastructure
		Decreasing of tax collection
		Jeopardy of state prestige

Resource: Own

4.2.3 Classification of cyber conflict costs according to time character costs (preventive and an eliminative character of costs).

Typ nákladů	Popis dané kategorie nákladů[34]
Krátkodobé	Náklady související s obnovením napadeného systému do stavu před napadením
	Náklady související s narušením činnosti organizace (ztracená produkce, neodbavení klienti ...)
	Pokles hodnoty nehmotného majetku (duševního vlastnictví) atakovaného během konfliktu
Dlouhodobé	Nárůst nákladů kybernetické bezpečnosti
	Ztráta klientů, obchodních partnerů,
	Dominový efekt provedení kybernetického útoku

Resources: Own

CONCLUSION

Cyber space becomes real security threat (it is prove empirical and theoretical evidence).

Crucial problem is determination optimal level expenditures and paid costs of securing sufficient level of cyber security and defense.

The question is what potential damages can impose real cyber-attack on society, individuals and firms.

It is necessary to find efficient way how to face this risk.

Society has to tolerate acceptable level of private and public costs on securing sufficient level of cyber security and defense.

TASKS FOR SELFSTUDY

1. Describe historical development of cyberspace research and try to explain why and when does cyberspace become 5th domain for armed forces activities. Define the meaning of Cyberspace, cyber conflict and cyber-attack.
2. What basic economic principles can we use for research of cyberspace and cyber conflict?
3. Explain the basic approaches to economic analysis of cyberspace as new security threats. Which research levels can we demarcate and describe?
4. Try to find case studies and examples of real cyber-attacks. Try to accomplish its economic analysis.

REFERENCES

1. GORDON, Lawrence A., LOEB Martin P. The Economics of Information Security Investment, 2002
2. BAUER, Johannes M., Van EETEN, Michel J. G. Cybersecurity: Stakeholder incentives, externalities, and policy options, 2009.
3. CORDES, Joseph J. An Overview of the Economics of Cybersecurity and Cybersecurity Policy, 2011.
4. DEPARTMENT OF FINANCE AND SERVICES. A Guide for Government Agencies Calculating Return on Security Investment, 2012.
5. CHIRCA, Alexandra. An Empirical Study Regarding the Cost-Benefit Analysis of Open Source Software for Information Security, 2010.

ADITIONAL STUDY RESOURCES

1. VAN TUYLL, Hubert., BRAUER, Jurgen. Colonizing Military History: A Millennial View on the Economics of War. Accessible on: http://www.stonegardeneconomics.com/pubs/2003_vanTuyll_Brauer_DPE_v14n3.pdf
2. FRIEDMAN, Allan. Economic and Policy Frameworks for Cybersecurity Risks. Accessible on: http://www.brookings.edu/~/media/research/files/papers/2011/7/21%20cybersecurity%20friedman/0721_cybersecurity_friedman.pdf).

FOR BETTER UNDRSTANDING PROBLEM

For deeper understanding of problems and introduction into economic background is recommended to acquaint yourself with following extract of document about economic aspects of cyberspace (or to download this whole material from following website: http://www.brookings.edu/~/media/research/files/papers/2011/7/21%20cybersecurity%20friedman/0721_cybersecurity_friedman.pdf).

Economic and Policy Frameworks for Cybersecurity Risks

Allan Friedman

Cybersecurity as an Economic Problem

Cyberspace may be a new domain, but it is composed of systems, networks, and the protocols and standards that allow data to flow efficiently and meaningfully. Each of these systems and networks is ultimately under the control of a set of actors who choose to take specific actions regarding the security of the network. Similarly, the agreed-upon standards that run the network, from the IP protocol up through the mechanisms by which banks settle accounts in a credit card network, are the outcome of processes with stakeholders and influencers. These stakeholders, too, can choose to take specific actions. The economic approach to information security focuses on the incentives of these actors, and whether these incentives align with a socially optimal level of security. This security exists to counter bad actors, who have their own incentives. This section explores the incentives of attackers and defenders, and explains some distortions in the market for security that inhibit investment and behavior to reduce risk.

The attacker's incentives

During the first major wave of rapidly spreading malware, observers marveled at the damage done by internet worms such as ILOVEYOU, Code Red, and Blaster, as they flooded networks with copies of themselves. Observers also noted the fact that many of these worms did remarkably little damage to the host machine, they simply spread. The creators were apparently not seeking any noteworthy gain beyond introducing something large and destructive into the internet ecosystem. Today, however, most attackers seek to gain something. Whether it is to destroy a system, obtain valuable intellectual property and data, or old fashioned profit, one can model today's cyberthreat as an actor seeking some goal.

The natural question, then, is what that goal is, and how important is the realization of it? If we can understand how much the cyber-adversary would pay in time, effort, acquired expertise, and expenditure, we can better understand an approach to defense.
In the national security context, the obvious goal is the disruption of systems. As discussed above, much has been written on the myriad ways a well-equipped and well-informed attacker could inflict grievous harm on any society dependent on information technology. National security, of course, is a high priority for any country, and there is every reason to expect a large willingness to pay for offensive capacity.

One can expect a similar approach to intellectual property, although here one might make some assumptions about the rationality of the attacker. The intellectual property has some value to the attacker, and hence, the budget would be a function of this value. We can even begin to put upper bounds on the expenditures of cyber exfiltration costs, since a determined adversary could obtain company secrets through other means, such as bribing an insider.
In both the national security case and the espionage case, one must assume a reasonably large budget of the attacker. This includes a key component: the intelligence budget. This includes the ability to value and even stolen data, or the expertise to know which systems to target. The attacker must have considerable knowledge of what he is trying to do, and how to execute it well, particularly if he wishes to minimize the risk of detection.

Incentives in cybercrime

There is a greater understanding of the economics of crime, particularly when one assumes financial motive. What is noteworthy about much of cybercrime is the small ratio of attacker's profit to damage. In one recent case, the United States Secret Service apprehended an individual found in possession of over 300,000 credit card accounts, which have been linked to some $36 million in fraud. Yet the best estimates in the criminal filing claim that "In all, the defendant personally received over $100,000 from his credit card fraud scheme" (United States vs. Hackett, 2011). While this is hardly a pittance, this is not an astronomical sum. Estimates vary on the value of credit card information on the black market, but the low end is almost always less than one dollar for a usable credit card number and expiration date, while the upper estimates seldom rise above a few tens of dollars (e.g. Moore, 2009; Symantec, 2011; Panda Security, 2011).

The low returns to those who steal account information have roots on both the supply-side and the demand-side. Ironically, the large numbers of credit card account information stolen drives down prices in a competitive market. The demand-side of this market must, in turn, find some mechanism of extracting value from these stolen account credentials without alerting active fraud detection mechanisms or compromising their own identity. A complex ecosystem has emerged to launder money through networks of handlers and mules. Much of this requires at least some manual intervention, raising the scaling costs.

Can criminals be deterred? Laws have been passed, with a renewed attention on inter-agency and international cooperation. Recent cases have demonstrated that law enforcement can achieve a non-trivial level of success in investigating and pursuing attackers. However, the jurisdictional issues and anonymity afforded by internet technology can impede investigations, and give attackers a sense of immunity to continue attacks. Moreover, it is important to remember that few law enforcement regimes successfully deter all crime. The international nature, and fluid nature of many online crimes make it difficult to engage in enforcement models specifically designed to deter crime, such as those described by Kleiman and Kilmer (2009). As the stakes rise to espionage or international conflict, the incentives to invest in clandestine activities that preclude attribution become greater. Disincentivizing attacks through enforcement and deterrence shows little promise.

We do, however, have one data point in favor of the efficacy of international law enforcement cooperation. Wang and Kim (2009) found that cyber-attacks originating from countries that have recently joined the Council of Europe Convention on Cybercrime fall between 15 percent and 25 percent. While this reduction could be explained by direct cooperation between signatory states, it is also possible that joining the treaty is indicative of a broader effort to take cybercrime more seriously.

Modeling attack and defense

Any model of even slightly sophisticated attackers must include a feedback mechanism where attackers are expected to adapt to defenses. Real-world evidence supports this. Phishing gangs switched from using domains registered in Hong Kong (.hk) to domains registered in China (.cn) as the Hong Kong Authorities became more proficient in shutting them down quickly (Moore and Clayton, 2007). Similarly, Day, Palmen, and Greenstadt (2008) show that websites hosting malware shift to more lax hosting providers as enforcement incentives are brought to bear. There is even evidence that state-sponsored espionage is adaptive. As government agencies step up their information security practices, American scholars and academics have come under attack from those seeking access to their emails and personal files.

Understanding the attacker can aid in better understanding defense. Bohme and Moore (2009) begin with an assumption that the attacker will begin by trying to compromise the weakest link in the defenses, although they do not expect the defender to know which component is the weak link. Following from these assumptions, they show that under certain circumstances, a rational defender would use the attacker to identify the important components in her system to strengthen and reinforce. In a dynamic game, the defender can continually raise the cost to the attacker while minimizing her investment in security.

Investment in security

On the defensive side, we must begin with the assumption that organizations can invest resources and effort to gain some benefit of security. Absent this assumption, the game is already over, and we can only focus on damage control. Below, we explore why actors might not be properly incentivized to invest in security, but first we must understand what security investment looks like, and how to think about the optimal level.

We can draw a distinction between two approaches to investing in security. In the first case, firms respond to existing threats, but do not proactively seek to address their exposed risk. This reactive posture is quite common: companies only invest in data loss prevention systems, for example, after they have lost data, or have reason to believe they may be at serious risk. They do not internalize the risk. In this case, investment will often only occur after harm has been done, and or in the face of future projected harm, such as the risks of lawsuits, or to improve a reputation.

Grossklags, Christin, and Chuang (2008) argue that this approach can be rational and even socially optimal. They frame it as a question of self-insurance, and show that it is sometimes advantageous. Returning to the question of data loss, there is evidence that suffering a breach has a small but significant impact on a company's share price (Acquisti, Friedman, and Telang, 2006). Yet this risk might be smaller than a systematic attempt to prevent potential breaches. The challenge here is that covering one's expected expenses of a security incident through self-insurance does not address any negative externalities that might arise. Investing in protection, on the other hand, reduces the overall likelihood of an incident, and thus can be viewed as a public good.

In this alternate model, firms or agencies can seek out particular security features. This is more common in industries that are regulated, where security features are mandated by law. In this case, security investment is legal compliance. Rowe and Galleher (2006) neatly frame the contrasts between prophylactic investment and responsive investment as two complementary investment functions. The reactive approach involves a decision to throw some amount of money to fix a problem: maximizing the security gained for a given budget constraint. The proactive security paradigm seeks to meet a specific security goal: minimizing cost subject to a specified security goal.

The impetus to invest more in security depends on the context, of course. In general, it can be internal, from a security-focused corporate culture or leader, to the needs of businesses (such as Amazon building a network resistant to Denial-of-service attacks), or in reaction to past breaches of security. Alternatively, the motivation could come from external regulations, or client demand.

Vendors are not insensitive to demand for security, but that demand is often tempered by clients who seek other features and lower prices, which can come at the expense of security. In the software, hardware and IT services markets, offering new features and being the first to the market is key. A first-mover advantage can translate to greater sales, not just for a given generation, but future sales and support costs through technical lock-in. Adding security features and engaging in rigorous pre-release testing adds time, complexity and cost to the vendor. As such, vendors often invest in security through consistent maintenance via patches to newly discovered vulnerabilities.

There has been a great deal of analysis on the optimal means of discovering and disclosing vulnerabilities. A market for vulnerabilities or "bug bounties" can increase the likelihood that the vendor will patch before an attacker will exploit a vulnerability, as long as the vendor patches in a safe and timely fashion. Since rapid patching has its own costs, a vendor may not rush to address the risk, thus exposing users to potential harm. Because of this, some advocates prompt public disclosure of vulnerabilities, while others maintain that information about vulnerabilities should not be disclosed until developers have had a reasonable opportunity to diagnose and offer fully tested patches, workarounds, or other corrective measures.

Market failures in cybersecurity

Given the high level of risk from the constant threat of attackers, why don't we see more investment in security? In an optimal world, the market would demand more security, and the builders and maintainers of systems to invest more. There are several reasons why one would not expect the market for security to function well. There are abundant negative externalities, poor information and predictable behavioral reasons why market actors may not be expected to invest in socially optimal levels of security.

To begin with, the very nature of networked technology offers some insights into the dynamics of cybersecurity markets. Information technology often yields its greatest benefits when everyone uses the same standards and platforms to maximize interconnectivity. Referred to as the "network effect," this phenomenon predicts that the value of a particular technology increases as the number of users increases (See Economides, 2007 for a survey of the network effect applied to IT).

While this is usually framed as a positive externality, since each adopter adds value to others, there are negative components. First, the network effect predicts the rise of dominant systems. As fewer systems and networks become integral to the infrastructure, it makes them more valuable to an attacker. Geer draws the parallel to the ecological risks of monoculture (Geer, 2003). For example, if a Facebook account now is a major source of interpersonal communication and allows comments on other websites and, a compromised account can be used for targeted phishing attacks and comment spam.

Many dominant products, including operating systems and social networks, are built to support a platform for other products. Other firms can provide innovative, complementary goods and services to enhance the value of these platforms. The original product designer has an incentive to make it as easy to develop complementary products. Imposing security requirements or building security into the platform from the beginning can serve as an impediment to the developers of these complementary products.

Finally, the network effect can amplify the barriers of entry for newer, more secure products, since switching costs include the forgone value of the old network. Even adding new security components can be difficult if it requires individual decisions. Many security innovations, such as DNSSEC, yield their benefits to the entire network. There is little incentive to be the early adopter, since network security products often do not improve overall security until other users adopt them. Indeed, products that are not subject to network externalities and offer benefits to the early adopters, such as SSH and IPsec, are more likely to succeed and diffuse quickly (Ozment and Schechter, 2006).

In general, if someone is responsible for protecting the system while someone else bears the cost of failure, then we might expect to see more failures. Economists refer to incidents when the social harms of a given action differ from the private costs of the transaction as "externalities."Pollution is a commonly used example of a negative externality, since the actions of the producer affect others in a way not reflected in the price. When individuals allow their machines to be captured by botnets that can be part of malicious activity against a third party, they are not internalizing the harms of failing to protect themselves. Unpatched vulnerabilities could be seen as a negative externality. So too are data breaches that harm the data subjects more than the breached party.

Externalities can arise from the expectations of others. Schelling cites the perverse incentives for helmets in hockey as an example where competition prevents socially optimal behavior (Schelling, 2006). He noted that while no player would voluntarily choose to wear a helmet, believing it imposed a slight disadvantage, most players were in favor of everyone wearing a helmet. Similarly, even though few market players would choose to invest in security at the expense of their competitive edge, it is quite possible that everyone would be better off with higher-levels of investment.

Finally, the market for security is fraught with information asymmetries that prevent optimal decision-making. Anderson (2001) helped launch the field of economics of information security by observing that the market for security products paralleled Ackerloff's (1970) market for lemons, or bad used-cars. Buyers are unwilling to pay for what they cannot measure. Producers are therefore unwilling to invest in producing security, but will still assert the security of their products. Like an untrustworthy used car market, bad security products will drive out good ones. Standards have emerged to certify that products do indeed meet specific security requirements. To be certified, the dominant practice is for the vendor to bear the costs of evaluating the product. This can introduce perverse incentives, where the vendor will seek out evaluation firms with whom it can negotiate "sweetheart deals". (NAP, 2007)

Even in good faith, it is very difficult to measure the effectiveness of a defensive measure. And when they can be adequately and simply verified, the product will, more often than not, close one vector of attack without precluding threat via other vectors. As such, a defender would only rationally expend some fraction of the value of a loss for a narrow defense, since risk still remains.

While different aspects of cybersecurity involve a wide range of incentives and economic forces, there is ample evidence for a market failure in security investment. What policies can use these same economic forces to promote better social outcomes?