Research Statement

Ghita Mezzour (mezzour@cmu.edu)

Cyber security has both technical and social dimensions. Understanding and leveraging the interplay of these dimensions can help design more secure systems and more effective policies. However, the majority of cyber security research has only focused on the technical dimension. In my research, I use a socio-technical approach that combines big data techniques, computational models, and network science methods. In my thesis, I studied factors behind international differences in cyber attacks, assessed countries’ cyber warfare capabilities, and simulated spam diffusion in social networks. These research interests have evolved from my past work on designing cryptographic protocols. Going forward, I plan to continue using a socio-technical approach to investigate factors behind international and temporal variation in cyber attacks and to study cyber threat perceptions. This future work will help customize systems and policies to better meet the needs of different countries and different communities.

Current Research

Global Cyber Threat. In some countries, computers encounter disproportionate quantities of cyber attacks, while in other countries computers host disproportionate quantities of these attacks. Empirically identifying factors behind such phenomenon can provide a sound basis for policies to reduce attack encounters and hosting. In previous work, however, identifying these factors is mainly based on expert opinions, not statistical evidence.

I built statistical models [13] that explain the international variation in the number of attacks encountered and hosted. I used the Symantec Intrusion Prevention System (IPS) telemetry data collected from more than 10 million Symantec customer computers worldwide, and combined that data with an attack description database [12] that I built based on Symantec online attack descriptions. The IPS data mainly cover web attacks, fake applications, and exploits. I used regression analysis to estimate the effect of countries’ wealth, cyber security expertise, corruption, web usage, and international relations on the number of attacks encountered and hosted.

My research has shown that Western European and North American countries encounter disproportionate quantities of attacks because these countries are rich, thus attacks on these countries are very lucrative. Moreover, my research has found that the combination of widespread corruption and reasonable computing resources in Eastern Europe creates a favorable environment for hosting cyber criminal infrastructure. This finding has significant policy implications. For example, making the environment in Eastern Europe less favorable to hosting cyber crime infrastructure requires a focus on cracking down on corruption. Other interventions such as providing cyber security training and increasing cyber crime penalties are unlikely to be effective and may even be counter productive; often, when corruption is widespread, increasing penalties may increase the crime rate [10, 7].

Cyber Warfare Capabilities. Many countries have included cyber security units in their militaries and announced their intent to develop cyber warfare capabilities. Assessing countries’ cyber warfare capabilities has important international policy implications, but prior work on assessing such capabilities consists mainly of case studies. Unfortunately, case studies require substantial expertise and effort and are difficult to perform for all countries.

I developed a computational methodology [4] and populated the methodology using real world data in order to estimate countries’ cyber warfare capabilities. My methodology examines all countries in the world and can be used by non experts. I leveraged the fact that the strength of countries’ cyber warfare capabilities depends on countries’ motivations for these capabilities and countries’ latent abilities to develop such capabilities. I developed a socio-cultural model to assess countries’ motivations and identified metrics to assess countries’ latent abilities. More specifically, I adapted the Friedkin socio-cultural model [5] in order to capture factors that motivate countries to acquire such capabilities. I then populated the model using publicly available data.
on international relations and the list of countries that have incorporated cyber warfare units in their militaries. Subsequently, I ran the model in order to obtain an estimate of countries’ motivations. Finally, I estimated countries’ latent abilities by examining the strength of cyber security research, the existence of cyber security institutions e.g. Computer Emergency Readiness Team (CERT), and information technology penetration in these countries.

The validity of my methodology stems from the fact that the methodology captures expert opinions and uses real world data. A further validation of the methodology would require comparing the methodology’s estimates to expert estimates. Although I did not perform that type of validation in the context of cyber warfare capabilities, it is worth noting that I performed that validation for a similar methodology [14] that I developed for predicting biological weapons proliferation. The biological weapons proliferation methodology had very high accuracy despite the fact that I only used publicly available data to populate the methodology.

**Spam Diffusion in Social Networks.** Spammers often use compromised email and social media accounts to spread spam. Such spam may promote scams, or may contain erroneous political information or advertisements for counterfeit products. However, prior work mostly overlooked modeling spam diffusion where compromised accounts are part of the diffusion. Previous research mainly focused on developing techniques to identify malicious accounts and modeling information diffusion in the absence of compromised accounts.

I modeled and simulated spam diffusion when compromised accounts initiate this diffusion [11]. More specifically, I modified a well established Agent Based information diffusion model [2] in order to capture the behavior of compromised accounts. Compromised accounts aggressively send spam to friends of the owners of these compromised accounts. These friends think the spam content is correct and forward the spam to their friends with a certain probability.

I found that modeling the behavior of compromised accounts causes spam to reach more people faster. More interestingly, I found that parameters such as spam credibility, the number of accounts initiating the diffusion, and the network size affect spam diffusion dynamics differently when the behavior of compromised accounts is modeled. These results, which received media attention [6], indicate that leveraging techniques from both the social network community and the cyber security community can provide a better understanding of the behavior of attacks on social networking platforms.

**Past Cryptographic Research**

Prior to addressing socio-technical dimensions of cyber security, I developed cryptographic protocols for sensor networks [8], vehicular networks [16], and social networks [15, 3]. When designing these protocols, my goal was to accommodate system constraints of the technologies involved. Later on, I realized that accommodating social conditions is an equally important goal that is often overlooked.

Sensor networks have stringent energy requirements. Prior secure sensor network communication protocols achieve high secrecy at the expense of high energy consumption (ZigBee), or low energy consumption at the expense of low security (TinySec). MiniSec [8] achieves the best of both worlds: high security and low energy consumption by leveraging the fact that computation consumes less energy than network transmission.

In vehicular networks, vehicles need to obtain Certificate Revocation Lists (CRLs) in a timely manner in order to avoid attacks by malicious nodes. Unfortunately, CRLs are large, and vehicles have low bandwidth and intermittent connectivity. Previous work did not address the efficient distribution of these CRLs. I developed a technique [16] that allows vehicles to receive CRLs within minutes while utilizing very low bandwidth. Such technique leverages Fountain codes [9], which are codes that transform a file into an unlimited number of encoded pieces such that the original file can be recovered from any sufficiently large subset of these encoded pieces.

**Future Research**

In the future, I plan to continue studying the interplay of social and technical cyber security issues with the goal of designing more secure systems and more effective policies. Below are examples of research directions I am interested in pursuing.

**Global and Temporal Cyber Threat.** In my prior work [13], I empirically tested the validity of expert opinions about factors behind international variation in network based attacks. A natural next step is to cover
a wider range of attacks by analyzing other data sets available through the Symantec WINE infrastructure. For example, the reputation data set, which contains 300 billion+ records about binary executables downloaded by users worldwide, are valuable for studying zero day attacks. I also intend to perform lower granularity analyses such as examining individual malware families and examining Internet Service Providers (ISPs). For instance, I will examine the relationship between malware families’ characteristics and socio-economic characteristics of countries where these families are most prevalent. Furthermore, I will investigate factors behind temporal variation in cyber attacks. I will also study cyber crime forums from Eastern European countries that disproportionately host attacks to gain a better understanding of the cyber crime environment in these countries.

This project will draw on a variety of methodologies that include network analysis techniques, statistics and machine learning. In the long term, this work will help customize security products and policies to better meet the needs of end users worldwide. In the interconnected world in which we live, reducing cyber security risk globally is critical to reducing such risk on a local scale.

**Cyber Threat Perceptions.** The way people perceive cyber security threats affect how these people address these threats. Unfortunately, different communities typically have different perceptions leading to major disagreements about how to address these threats. An important step towards resolving these disagreements is to understand unique perceptions. Through this process, we can identify areas of alignment.

In this project, I plan to characterize cyber threat perceptions of industry, government, end users and researchers. I will analyze cyber security discussions in social and traditional media as well as cyber security research. I will use network analysis techniques to identify concepts, entities and technologies that different communities consider important to cyber security. I will also apply sentiment analysis to gauge the tone of cyber security discussions within different communities. Lastly, I will examine the temporal evolution of such perceptions, and the temporal relationships between the perceptions of different communities. I expect this research to identify approaches to better meet the cyber security needs of different communities.

**References**


