HOW DO YOU CREATE A WORLD FINANCIAL COMMUNITY THAT IS RESILIENT IN THE FACE OF CYBER-SECURITY, CYBER-ESPIONAGE, AND HACKING?

Biographies of Authors

William Abbott Foster, PhD is a Senior Research Associate with the Center for International Strategy and Policy (CISTP) at the Sam Nunn School of International Affairs at Georgia Tech in Atlanta, Georgia. He has twenty-five years of experience in government, industry, and academia building global collective intelligence systems to support engineering policymaking including around cyber-security. His books and articles are available on-line at http://www.fosterandbrahm.com.
He can be reached at william.foster@inta.gatech.edu.

Hannah Thoreson runs a company specializing in social media research. She has a bachelors degree in physics from Arizona State University, where she interned for NASA Space Grant for two years. She has experience working in politics, public relations, and marketing.

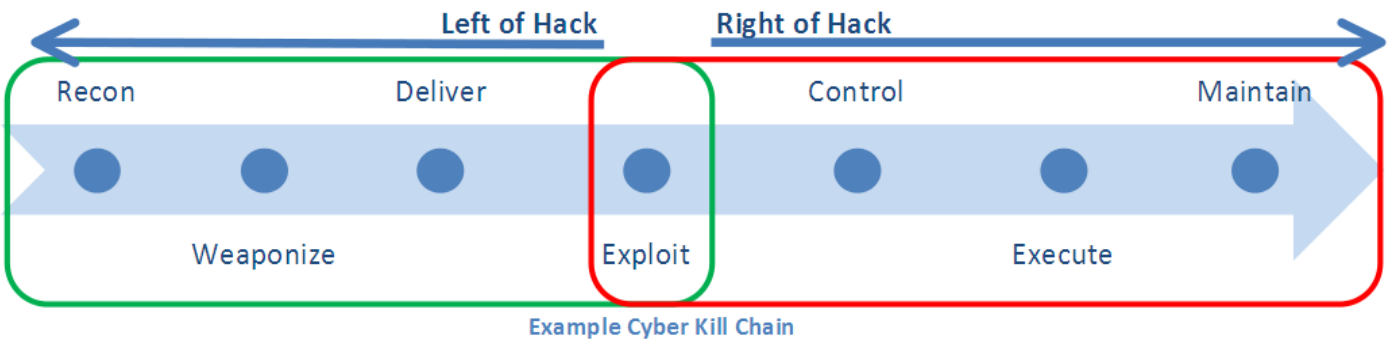
Introduction

What are the actual financial losses suffered by the world financial community in 2012 from hacking? How much of this was due to the Russian *cyber-mafia*? Are we on the verge of cyberwars between the US-Iran or U.S.-China and what might be the potential dollar impact?

Effective cyber-defenses require trust between governments and between governments and business? More effective defenses assume higher levels of trust for automated threat sharing, but increased threat sharing also increases one`s vulnerability to new kinds of targeted threats from those with who have learned about your weaknesses.

We have moved from a simple world where a threat could be detected by a signature downloaded from an anti-virus firm like Macafee or Symantec and neutralized.

Now attackers will now probe thousands of network simultaneously with thousands of different attacks a second looking for an exploitable vulnerabilities. These attacks are far beyond the capability of human operator to identify, isolate, and respond to such attacks or to let those they trust in government and industry to know about the attack in a timely (sub-second) window.



Example Cyber Kill Chain

Source: "*Standardizing Cyber Threat Intelligence* Information with the Structured Threat. Information eXpression (STIX™)," MITRE Corporation, July 2012

The first step in building an automated defense to current threats, is to make the threat information software and hardware independent. The U.S. government think tank MITRE under contact to the US Department of Homeland Security has developed an XML based system for automatic structured threat information called STIX.

If you are interested in STIX it is highly recommended that you read MITRE's "Making Security Measurable" white paper available at http://makingsecuritymeasurable.mitre.org/docs/STIX-Whitepaper.pdf Mitre has developed a website for conveying developments about STIX. It is at http://stix.mitre.org/.

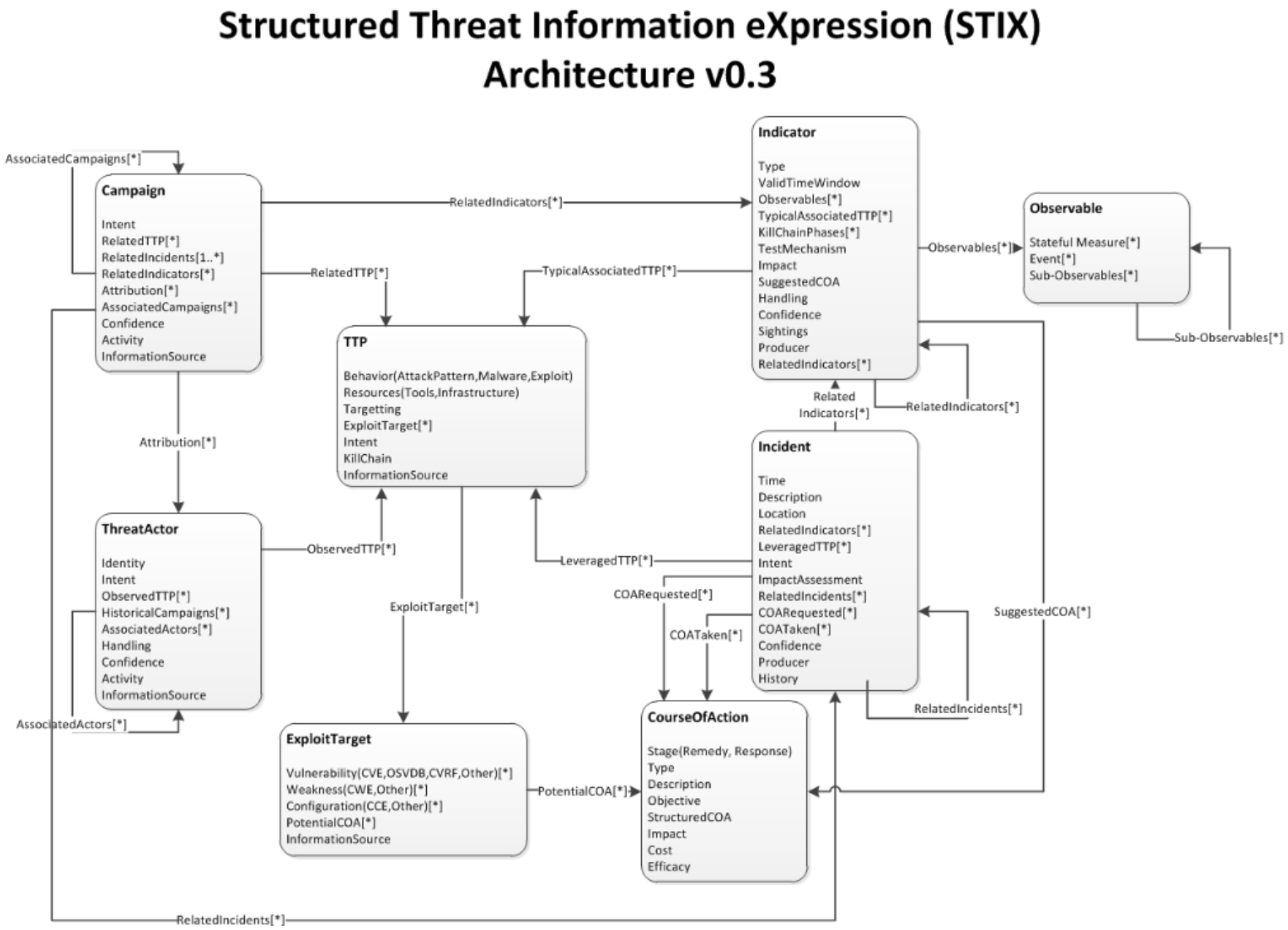
MITRE has a long history of developing sophisticated security technology which though technically sophisticated is often never fully adopted by industry. We believe that our society faces a major cyber-security challenge, a challenge that US policymakers cannot address by focusing on US cyber-infrastructure. For example, the world's financial community is under widespread cyber-attacks that come from all over the world and require a global response.

Functionality of STIX

STIX, or the Structured Threat Information eXpression, is a language "meant to convey the full range of cyber threat information and strives to be fully expressive, flexible, extensible, automatable, and as human-readable as possible" (The MITRE Corporation, 1). At least at this point, STIX currently exists as a programming language within a programming language. It is a specialized XML schema that has been developed with the primary purpose of "tagging" various aspects of a successful or attempted exploit (MITRE, 5). The data can then be collected, shared, and used by systems or organizations using a common standard for formatting the information. STIX is practical, because it leverages existing standardized language where appropriate; for example, in its representation of observables, it leverages the CybOX standardization effort (MITRE, 12). It also is designed such that everything in STIX is optional for the end user.

STIX "is intended to provide full expressivity for all relevant information within the cyber threat domain". As such, it is designed to be helpful when performing a wide range of tasks, as opposed to emphasizing only a narrow band of the cybersecurity realm. For example, STIX is useful for analyzing

cyber threats, because it has a structured, standardized way to find and collect the data on an attack. It is also helpful in specifying indicator patterns for cyber threats, taking preventative courses of action for relevant threats, monitoring cyber operations, and responding to incidents (MITRE, 8). STIX is also extensible in case a user finds its toolbox to be incomplete (MITRE, 10).



Source: "*Standardizing Cyber Threat Intelligence* Information with the Structured Threat. Information eXpression (STIX™)," MITRE Corporation, July 2012

The way STIX achieves these goals is by identifying the data objects that could be collected about an attack, and then fleshing out those constructs in detail within the XML schema housing the language (MITRE, 11). The eight "core constructs" that MITRE identified when developing STIX are the Observable, Indicator, Incident, TTP (Tactics, Techniques, & Procedures), ExploitTarget, CourseOfAction, Campaign, and ThreatActor (MITRE,11). STIX leverages existing standards when defining observables and indicators. However, it develops its own language for all or part of the other core constructs as no adequate standards currently exist.

STIX and Trusted Relationships

Trust is extremely important in cybersecurity in order to enable sharing of information about threats and security breaches between institutions. Unfortunately, there is a major lack of trust between corporations, between the private sector and government, and between U.S. organizations and those belonging to countries outside the West. Companies often like to keep security information private, as making their vulnerabilities known may cause them to lose customers (Bipartisan Policy Group, 2012, 9). There are also legal concerns surrounding information sharing in the U.S (Bipartisan Policy Group, 2012, 9). Data must be handled in a way that respects consumers' privacy and civil liberties (Bipartisan Policy Group, 2012, 5). Companies are also often loath to collaborate with the government, which makes it difficult for security agencies to develop practical strategies for protecting U.S. infrastructure (Harwood, 2011). All of this is to say nothing of the borderline-hostile relationship between U.S. cybersecurity agencies and their foreign counterparts, which creates an environment that is not at all conducive to sharing information about threats and attacks.

These drawbacks are some of the reasons that in the past, MITRE has developed other cybersecurity products which never saw much practical use. These products may be very technologically advanced but ignored by private industry. Part of the reason for this may also be that private industry is often reluctant to inorganically adopt a new standard. One of the most popular language in private-sector software development is still C++ and Java. Since so many programmers learn and are trained in the most popular languages and procedures, there has been a surprising resistance to moving to an XML orientated strategy for ensuring that data is hardware and software independent.

President Obama - President Putin - President Xi Ping

Given the present risk that the world`s financial industry faces, one would think there would be a lot of interest in deploying STIX. However, we have interviewed four cyber security experts in the Chinese financial industry. All agreed that they had no interest in a cybersecurity solution like STIX that was developed by the US government. We were told that only if President Obama approached President Xi Ping about working together on a global cyber-security solution for the world`s financial community, would China implement STIX.

Though Americans deeply distrust Chinese hackers, it must be remembered that Chinese hackers are not allowed to hack "credit card information from the west", because credit card information is the turf of the People`s Bank of China. Through its sophisticated firewalls, the Ministry of State security tracks every international hacker in China.

The Chinese government has the technical ability to stop all attacks against the world`s financial community and if President Obama asked in he right the PRC government could take a lead in building "trust" relationships between Chinese financial institutions and the rest of the world.

The Russian cyber-mafia is one of the greatest threats to both the American and world banking systems and take advantage of the lack of automated threat sharing in the community. With the support of

President Putin, President Obama and President Xi Ping could drive the leaders of the world`s financial industries to engage in trust building exercises that would lead to the world wide implementation of STIX and artificial intelligence systems built on top of STIX. Though such an effort requires a baseline of trust, the world wide implementation of STIX would greatly strengthen relationships within the world financial community and the degree of trust in the community.

More importantly if the US, China, and Russia invest heavily in the resilience of the world`s financial community they come to common agreement to make sure that any of their cyberwar attacks do not touch the world's financial system.

In this article we argue that the Obama Administration should take the lead and have the US Department of Treasury reach out to the Chinese Banking and Regulatory Commission and the Peoples Bank of China to work together to make the world's financial system more resilient. The US government has funded the development by MITRE of a system for automated threat exchange to support critical US infrastructure. This XML based system has been presented to the Internet Engineering Task Force (IETF) at their Fall meeting in 2012, should be implemented quickly at a global level by building on and contributing to "trust" relationships in the world financial community, particularly the relationships between US and Chinese financial leaders.

24.04.2013