Congressional Testimony

A Global Perspective on Cyber Threats

Michael Madon
Board of Advisors Member
Center on Sanctions and Illicit Finance, FDD
Vice President, Business Development, RedOwl Analytics

The House Committee on Financial Services
Subcommittee on Oversight and Investigations

Washington, DC
June 16, 2015

Center on Sanctions & Illicit Finance
FOUNDATION FOR DEFENSE OF DEMOCRACIES
1726 M Street NW ● Suite 700 ● Washington, DC 20036

Chairman Duffy, Vice Chairman Fitzpatrick, Ranking Member Green, and other distinguished members of the Committee, it is an honor to appear before you to discuss the global cyber threats we face and in my view, more importantly, what we can do about it.

During my time at Treasury, I was fortunate to work for and with a team of true innovators developing novel strategies and approaches to identify and mitigate the cyber risks and vulnerabilities facing both the department and financial sector more broadly. More recently, I have worked closely with Juan Zarate, a visionary and founder of that early Treasury team and who currently serves as Chairman and Senior Counselor of the Center on Sanctions and Illicit Finance (CSIF) at the Foundation for Defense of Democracies. The thoughts below are inspired by our early Treasury work and taken in no small measure from Juan's current writings on this topic.

Five Primary Cyber Threats

While cyber attacks and intrusions threaten US private sector institutions on a daily basis, cyber attacks against financial services institutions in particular are becoming more frequent, more sophisticated, and more widespread. In my view, the rise in frequency and breadth of these cyber attacks can be attributed to five primary threats:

- First, nation states striving to steal intellectual capital from banks and/or destabilize them;
- Second, cyber terrorists seeking to disrupt and destroy the transactional glue that binds our community of nations and who view our financial institutions as symbols of Western capitalism.
- Third, "hacktivists" who make opportunistic attempts to break into banks' IT networks, to draw attention to some cause or deeply held belief.
- The fourth are organized crime elements who breach systems for monetary gain.
- The fifth is the insider threat. In its most recent Data Breach Investigation Report, Verizon provided the following observation on all security incidents reported in 2014, "It may not be obvious at first glance, but the common denominator across the top four patterns - accounting for nearly 90% of all incidents - is people. Whether it's goofing up,

> getting infected, behaving badly or losing stuff, most incidents fall in the [user error category].” The uncomfortable truth here is that individuals that we bring inside the enterprise and trust with systems and data access are the root cause or unknowing enablers of most cyber incidents.

Threats against the Financial Community.

If the recent attacks against JPMorgan Chase & Co. and Citibank serve as examples, banks are prime, vulnerable targets for sophisticated, organized cyber attacks, despite a dramatic increase in cyber security spending. The frequency, sophistication, and breadth of attacks on banks are swelling in large part because banks hold not just money but also collect and centralize sensitive personally identifiable information and clients’ intellectual property.

Benjamin Lawsky, superintendent for New York’s Department of Financial Services, the city’s top banking regulator, said, “The cyber threat has to become urgent, one of the most important issues facing financial sector chief executives. It’s got to be at the chief executive level. It is not an IT problem. It is a bank problem.”

Further, banks have been pulled into a more serious and sustained cyber financial battle. The primary cyber threats realize that banks serve as both key systemic actors important for the functioning of the global economy and as chief protagonists in the isolation of bad actors from the financial system. Thus, the financial community finds itself drawn into combined financial and cyber battles – neither of which they control. As Juan Zarate has noted,

> “the conflicts of this age are likely to be fought with markets, not just militaries, and in boardrooms, not just battlefields. Geopolitics is now a game best played with financial and commercial weapons. And those weapons now include cyber tools, used by non-state and state actors alike to attack banks and financial systems. The new geo-economic game may be more efficient and subtle than past geopolitical competitions, but it is no less ruthless and destructive.”

Our society's current response is not sufficient to address growing cyber threats. We need to have a more pro-active approach, one that shifts the paradigm away from defense to offense. We can take inspiration from the anti-money laundering and sanctions model forged at Treasury and leverage financial pressure against cyber threats to better protect the financial system. This would entail a model to promote "Cyber-Driven Targeted Financial Measures" to empower and enlist the private sector to better defend its systems in coordination with the government.

A Snapshot of Current Private and Public Sector Partnerships

Collaboration between the public and private sector, and the financial sector in particular, is not new. But the process for sharing information among the private sector and with government has been slow and not automated – or has relied on reports that are rarely analyzed, as with the security violations filed by financial institutions with the Treasury's Financial Crimes Enforcement Network, as part of Suspicious Activity Reports. Collaboration has also relied on private sector threat intelligence services that do not necessarily communicate with others. But there are some diamonds in the ruff:

- The Financial Services Information Sharing and Analysis Center (or FS-ISAC) is the primary industry forum for collaboration on critical security threats facing the global financial services sector and has grown increasingly operational. For example, the FS-ISAC has recently teamed up with the Depository Trust and Clearing Corporation, which provides post-trade financial services, to launch a new software platform. Beginning with a pilot of 45 organizations, it will be used to share information about attacks and attempts at attack at a real-time speed intended to prevent hackers from deploying the same cyber weapons against several companies consecutively.

- The Treasury Department has tried to accelerate the sharing of timely and actionable cybersecurity information that financial institutions can use to defend themselves by establishing the Cyber Intelligence Group. This group works closely with the FS-ISAC to produce circulars and information in response to financial sector requests.

- Executive Order 13636 signed in February 2013 – "Improving Critical Infrastructure Cybersecurity" – gave rise to the National Institute of Standards and Technology's (NIST) Cybersecurity Framework, a compendium of best practices and security standards developed to perform risk assessment and mitigation, as well as encourage information-sharing between the private sector and government.

- In February of this year, President Obama signed an Executive Order to encourage and promote sharing of cybersecurity threat information within the private sector and between the private sector and government.

- Cyber analysts within the US Intelligence Community continue working to identify threats and disseminate information to the rest of government.

    - At the Department of Homeland Security (DHS), the National Cybersecurity and Communications Integration Center (NCCIC) is a 24-7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for federal government, intelligence community, and law enforcement.

    - The US Secret Service uses the Electronic Crimes Task Force (ECTF) to leverage the combined resources of local, state, and law enforcement with prosecutors, private industry, and academia to combat cyber criminal activity.

    - FBI's NCIJTF is its "next-generation cyber initiative" and serves as a coordination, integration, and information-sharing center for nineteen U.S. agencies and cyber threat investigations.

There is no dearth of attempts by the US government to try to increase information sharing with the private sector. Indeed, the private sector—including the financial industry—often feels bombarded by different government agencies attempting to gain access to information or serve

as the principal interlocutor for the government. The private sector also feels exposed without legislation to protect their activities. Indeed, all of these aforementioned models maintain a strict divide between public and private sector actors – often with liability and risk attached to those private sector entities willing to share information or openly divulge their vulnerabilities.

Further, under the current system, there is little incentive for pro-active defense of financial systems and legal restrictions on more aggressive monitoring and disruption in cyber-space by systemically relevant and important private sector entities. And so a new, more pro-active model should be considered as the financial industry finds itself in the eye of the cyber-storm and as the financial system is increasingly at risk from sophisticated attackers.

Cyber-Driven Targeted *Financial* Measures

A new economic and cyber security approach requires a new paradigm of US public-private engagement and collaboration. This involves an evolution from classic, state-based national security actions toward deeper involvement of and reliance on the private sector in arenas previously confined to the halls of government, with a commensurate and widening appreciation within governments of the private sector to influence international security.

As Juan Zarate notes, "the utility of this approach is that it is not based on private sector altruism or civic duty, but on the self-interest of legitimate financial institutions that want to minimize the risk of facilitating illicit transactions that could bring high regulatory and reputational costs if uncovered." Further, as certain verticals within the financial sector increasingly become commoditized, a robust program of public-private engagement and collaboration may become the discriminator - the edge -that drives profits.

These measures seek to:

- Encourage the creation of internal Financial Intelligence Units (FIU) to enhance financial sector and augment US Intelligence Community collection and analysis efforts. Many banks have already or are now establishing FIUs to analyze internal data and understand and manage financial crime and sanctions compliance risk. These systems complement

the cyber and technical defenses being built in all major financial institutions. Banks can build on these financial and analytic systems to better understand potential cyber intrusions and the transactions flowing through their systems.

- Enhance Safe Harbor Regime to Encourage Greater Information Sharing Among Financial Institutions. Secretary of the Treasury Jack Lew recently made the case for clearer rules of the road to allow for information sharing and protection of rights:

  "As it stands, our laws do not do enough to foster information sharing and defend the public from digital threats. We need legislation with clear rules to encourage collaboration and provide important liability protection. It must be safe for companies to collaborate responsibly, without providing immunity for reckless, negligent or harmful behavior. And we need legislation that protects individual privacy and civil liberties, which are so essential to making the United States a free and open society."

- Enhance Section 314(b) of the USA PATRIOT Act to allow financial institutions to share information about suspect cyber-related financial activity within their sector, without liability. This provision should be matched in the cyber intrusion and attack context, and there should be legal safe harbors for information sharing between and from private sector actors intended to inform or assist in cyber defense.

- Accelerate the US government's targeting of state actors, networks, and individuals that attack US private sector systems – especially financial systems. US law enforcement has consistently investigated cases of breaches, including of organized crime rings and hackers that successfully penetrate US-based systems, with indictments often following.

- Deploy the President's emergency economic powers for the use of multiple tools to address the reality of major cyber espionage, crime, and infiltration affecting the US financial and commercial system.
  - In the first instance, the President should sign a new executive order, based on his power under the International Emergency Economic Powers Act (IEEPA), that

would allow the Secretary of the Treasury, in coordination with the Secretary of State and the Attorney General, to identify cyber hackers, state sponsors, and those entities and individuals owned or controlled, who financially support such activities, or who are otherwise associated. This would allow the US government to use the tools of economic and financial isolation – including freezing assets and blocking transactions -- against those companies, entities, networks, and individuals identified as being behind major cyber attacks to include infiltrations, disruptions, and espionage.

- Encourage Congress to craft legislation to empower the Secretary of the Treasury to identify jurisdictions, institutions, or networks that are sponsoring or willfully allowing their territory or systems to be used to attack American financial institutions. As with the provisions of Section 311 of the USA PATRIOT Act regarding "primary money laundering concerns," the label of "primary cyber security concern" could be applied to any such actor and could bring with it a range of consequences and potential countermeasures against a jurisdiction's economy, including measures to sanction or bar from any business in the US those companies or entities found to be benefiting or profiting from cyber espionage.

Cyber-Driven Targeted *Active-Defensive* Measures

Innovative criminals require innovative responses and Congress could enlist the private sector in participating in a cyber-driven targeted, active-defensive measures that reward, enable, and empower the private sector to help defend itself in concert with government. This would require rule-setting, more active collaboration, and explicit line drawing and processes, but such a regime is imaginable. This model could be based on the tradition of congressional issuance of "letters of marque and reprisal," as provided for explicitly in Article 1, Section 8 of the US Constitution. Governments provided these letters to private merchant ships, granting them the authority and monetary incentive to attack and capture enemy vessels and bring the cases before admiralty courts. In the age of piracy and maritime insecurity, this was a legitimate method of providing maritime security in the early days of the Republic.

This model could take different forms to include:

- A Reward Program for those groups able to uncover, identify, and even "deliver" cyber hackers to US courts or authorities – as security groups have done in the past. Admittedly, attribution of activities carried out through the internet is extremely difficult and, in many cases, impossible to achieve. There is a large swath of grey among these groups – and the swath is just getting bigger. For example, tracing the line where a Russian hacktivist or organized criminal network ends and the Russian government begins can be dashed, missing, picked up again as a solid line, only to dissolve soon after into a suspicion or best guess. Yet, as the "attribution revolution" in the private sector – with ever better cyber forensic technology to identify the source of cyber attacks – begins to shed light on once opaque activities, the possibility of more aggressive tracking, detection, and targeting becomes a reality.

- Unleash the Power of Cyber Forensic Teams and Private Litigants and plaintiff's lawyers against those attacking US systems. Qui tam actions that allow private litigants to benefit from the identification of prosecutions should be designed to reward those building cases against cyber hackers and state sponsors. This would incentivize further those able to attribute attacks and would deputize the private sector and lawyers to investigate significant cases.

- Empower Victims of Attacks to Sue the Perpetrators and those benefitting directly from any cyber infiltrations, just as victims of terrorism are provided the right to sue terrorists, state sponsors, and terrorist financiers and facilitators. Thus, shareholders and companies could be given the right to sue those who have perpetrated, sponsored, or benefited directly and knowingly from cyber attacks. This would have the benefit of unleashing the power of the plaintiff's bar – focusing less attention on those attacked by the breaches and instead on those benefiting from the attacks.

- Encourage the US Department of Justice, Department of Homeland Security, and Treasury Department to consider issuing special cyber warrants – another type of "letter of marque and reprisal" -- to allow US private sector actors to track and even disrupt cyber attacks in certain instances to defend their systems. While this would not happen overnight and would require a defendable attribution regime and real-time capability to respond to targets of opportunity and evaluation of the negative externalities of any such action

The government today is in a position to enable the private sector – and even private individuals – to pursue active defensive measures on its behalf vis-à-vis a new model. Individuals would be given the resources necessary to bring suits against those who threaten their assets abroad and domestically. The burden of financial integrity would move from top-down federal control to a democratized, flattened system, and usher in a new era of financial warfare.

This could take directly from the model of the Financial Action Task Force (FATF), which is the international body comprised of thirty-six jurisdictions that sets international standards and norms on anti-money laundering, countering the financing of terrorism, and proliferation financing. The FATF, along with regional-style FATF bodies, elaborate these standards and practices and, along with the IMF and World Bank, assess countries on their implementation and effectiveness.

Committee members, thank you for allowing me to appear before you and discuss the global cyber threats. My colleagues at the Center on Sanctions and Illicit Finance and I look forward to collaboratively devising and implementing strategies to defeat the growing cyber-threats that confront our nation.