Statement Before the

House Committee on Financial Services
Subcommittee on Terrorism and Illicit Finance

"After the Breach: The Monetization and Illicit Use of Stolen Data"

A Testimony by:

James Andrew Lewis

Senior Vice President

Center for Strategic and International Studies (CSIS)

March 15, 2018

2128 Rayburn House Office Building

I thank the Committee for the opportunity to testify on this subject.

In the 1990s, when the Internet was commercialized, there was a strong millennial belief that this was part of a new age of peace and harmony, with the end of the Cold War and with what some went so far as to call the end of history. All countries would be market democracies, Russia and China would be friends, the role of government would shrink and be replaced by a new multi-stakeholder governance model, the boundaries between countries would fade and the Internet would be the glue that held this new world together.

Millennial optimism has proven to be badly mistaken, but it still undergirds some of our thinking about the Internet, such as the benefits of anonymity, often justified as essential for dissent, but which remains an immense benefit for criminals. The last few years have shown that the Internet has a dark underside that is deeply troubling. The Internet has brought tremendous economic benefit, but this comes with the costs created by espionage and crime. The loss per victim from cybercrime can be low, but there are many victims and the costs and risks of engaging in cybercrime are even lower, making this an irresistible criminal activity. The task for policymakers and legislators is to find a way to reduce that cost without sacrificing the Internet's benefits.

Cybercrime is big business. How big a business is a subject for dispute and, like so many things connected to information technology and the Internet, also a subject of imprecision, hype and exaggeration. CSIS has conducted three studies, with the support of McAfee, to estimate the losses from cybercrime. In interviews for our studies, one senior official called it "the greatest transfer of wealth in human history," while another, a member of the Council of Economic Advisors at that time, called it a "rounding error in a fourteen trillion-dollar economy." Through our work, we hoped to narrow the gap between these two extremes.

Our first study of cybercrime, done in partnership with Stewart Baker, attempted to establish upper and lower bounds for cybercrime by looking at other categories of crime for which there was available data, such as narcotics, maritime piracy, pilferage and (for an estimate to social cost) automobile crashes. This comparison let us estimate how much crime a society can tolerate as part of everyday life, and suggested a range of 0.5% to 1.5% of national income. For perspective, when you hear that cybercrime costs the U.S. a trillion dollars a year, this would be roughly 6% of national income, an immense sum unmatched by any other category of crime. We assessed this as unlikely.

Estimation of the cost of cybercrime is challenging because data collection is woefully inadequate. Even major economies do not collect statistics on cybercrime. This is somewhat understandable because many victims prefer not to report their losses. We tried to account for this in our estimate. There are also valuation problems in deciding how much stolen intellectual property is actually worth or what the market prices are for stolen personal information, a price that can fluctuate with supply. Additionally, there is no common definition on what should count as cybercrime. Some countries count anything where a computer is used. Others do not count intellectual property theft. Developing a common global standard of what should be counted and making the collection of data a priority would help us asses the scope of the

problem. Until then, estimates must do. This may change over time, as insurance companies collect actuarial data on cybercrime, or it may require government intervention in the same way we estimate the cost of narcotics-related crime.

One major difficulty for estimating the cost of cybercrime and cyber espionage is the problems that criminals face in monetizing the results of their theft. Even if we know the value of what was taken, in many cases criminals cannot gain the full value, particularly for personally identifiable information (PII) or intellectual property (IP). It is harder (in some cases, much harder) to monetize the result of a successful hack than it is to hack itself. One reason we believe that cybercrime continues to increase is that criminals have become better at monetization, in part because of the availability of cryptocurrencies like Bitcoin.

Monetization is easiest is when a criminal can transfer funds directly from the victim to a bank account. In the past, this was done by using "mules" or "cashers" to launder money extracted from breached accounts. Cybercriminals transferred stolen funds to the mules' accounts; the mules will take a "commission" (often between 5-10% of the total) and forward the rest to overseas accounts. These older processes were both risky and inefficient. The development of cryptocurrencies reduced risk and increased returns, by increasing the anonymity and ease of criminal transactions. The cybercrime monetization process is increasingly digitized, with criminals moving stolen funds rapidly among accounts with the goal of using it to buy cryptocurrencies in untraceable ways.

Business confidential information can also be monetized easily, by providing the criminal acquirer an advantage in business negotiations or an ability to conduct a transaction at a lower cost than would otherwise be the case. Accounting firms and law offices have become favorite targets for this category of cybercrime since many are small and not well protected. Advance information on quarterly results or mergers and acquisitions could allow a sophisticated criminal to take advantage of the market in ways that could be difficult to trace, making the manipulation of stock prices and other financial assets one of the more difficult aspects of cybercrime. This kind of financial manipulation avoids many of the problems related to monetization.

Monetization of stolen data, whether IP or PII, has always been a problem for cybercriminals. Digital currencies have helped to change that, but they have not solved the fact that there can be a broad gap between what cybercriminals steal and what they able to exploit. Criminals cannot monetize everything they take. Millions of individuals can lose their credit card data in a single incident, but only a fraction of those affected will experience monetary loss. Similarly, thieves and spies may take intellectual property that cost billions to develop, but they face real challenges in their ability to turn this IP into competing products. The gain from the crime to the criminals will vary from product to product depending on how easy it is to turn the stolen IP into a product that can be sold on the market. The theft of a formula for some product like house paint or furniture, for example, allows a competitor to begin production almost immediately. The theft of IP for high tech products like semiconductors, however, might not be useful at all without a modern industrial base that can manufacture products based on the stolen IP.

As an aside, this is part of the explanation as to why China has tried in the last few years to acquire semiconductor companies in the West. China's economic espionage actions before 2015

included the acquisition of IP related to semiconductors, but the Chinese, despite massive investment, lacked the "know-how" to turn the stolen IP in products. While the purchase of western companies has been blocked by regulatory tools, such as the CFIUS process, China's immense government investments and use of joint ventures will eventually allow them to them to overcome the "know-how" obstacle.

Our second report developed a model to estimate of the global cost of cybercrime, based on data from interviews with government officials in a number of countries as well as published and private data on nations' aggregate cybercrime losses. We found information on thirty-two countries that account for a significant portion of global income, and used this data to construct a global estimate for cybercrime. We looked at a broad range of costs, including recovery costs, damage to brand and liability, and opportunity costs– the value of opportunities or benefits that cannot be realized because resources have been expended to protect or recover from cybercrime. We estimated that in 2014 the global loss was between $375 and $425 billion a year.

Our third and most recent study used the same methods and refined this approach by looking at countries by income group (high, medium or low income, using World Bank categories). The study showed an increase in cost, and estimated that cybercrime cost the world between $450 and $600 billion a year, roughly a twenty percent increase. This increase can be explained by the increasing sophistication of cybercriminals, by the larger number of Internet users and volume of Internet transactions which increases the pool of potential victims, and by improvements in the ability of cybercriminals to monetize stolen data.

This improved ability to monetize stolen data is in good measure the result of availability of cryptocurrencies and the continued growth of cybercrime black markets in what some call the "Dark Web." The dark web, websites accessible only through special programs or networks like Tor, has created a space for sophisticated criminal markets and transactions to operate outside the reach of law enforcement and has made the Internet a central hub for global criminal activity in drugs, child pornography, arms, and malware. Cryptocurrencies are an essential part of these marketplaces, allowing transactions to occur with far less visibility than ever before. The development of the dark web and cryptocurrencies support the growth of a sophisticated cybercrime ecosystem, and have eased the challenges of monetizing the spoils of cybercrime.

Digital currencies are cumbersome to use for many transactions, fluctuate in value, and are not widely accepted by mainstream commercial vendors. In 2017, the largest daily amount of bitcoin transactions was around $5 billion. For context, data from the Bank of International Settlements suggests that $5 trillion is traded every day in currency trades. Bitcoin is a rounding error in global financial transactions. Perhaps someday this will change, but for now, cryptocurrencies are primarily a vehicle for currency speculation, online gaming, and for cybercrime.

The preferred currency for anonymous transactions remains the U.S. $100-dollar bill, with more than twelve billion bills in circulation according to the Treasury Department.[1] Cash is still preferred for crime and tax evasion, but for cybercrime, cryptocurrencies have an advantage by avoiding the need for cumbersome and detectable physical transfers or bank transfers subject to

[1] https://www.federalreserve.gov/paymentsystems/coin_currcircvolume.htm

regulation. The failure to counter the proliferation of unregulated digital currency exchanges, and the availability of strong encryption has created opportunities for cybercriminals, state-sponsored cybercrime, sanctioned governments, and terrorists as they effectively evade money laundering controls and find it easier than ever to move large sums quickly and anonymously.

Cryptocurrencies are the digital equivalent of cash, and can allow for untraceable financial transactions. Bitcoin has long been the favored currency for darknet marketplaces, with cybercriminals taking advantage of its pseudonymous nature and decentralized organization to conduct illicit transactions, demand payments from victims, and launder the proceeds from their crimes. Bitcoin's oft-cited anonymity is not perfect, however, which has led to the emergence of a new generation of privacy-enhanced cryptocurrencies offering far greater protection to help cybercriminals conceal the details of their transactions and evade law enforcement. There are dozens of different cryptocurrencies on offer world-wide. Transactions using cryptocurrencies are difficult to trace and once the cryptocurrency is obtained in the commission of a crime, it is relatively easy to use the Internet to transfer it to a bank and exchange it for fiat currency.

Monetization opportunities have also increased due to the flourishing black markets found in cyberspace. Encryption, the dark web and cryptocurrencies have created a safe haven for cybercrime. These black markets are not accessible from the visible Internet, nor can they be discovered by widely used search engines. Access to these markets is usually restricted. On them, you can buy the latest hacking tools or recently stolen PII, learn of recently discovered vulnerabilities, and rent "botnets" --tens of thousands of computers remotely controlled for criminal purposes, usually used for conducting denial of service attacks or engaging in cryptocurrency mining. These black markets can be highly specialized. Some sellers offer guarantees, product ratings, and customer service. Personal information - credit card numbers, social security numbers, and bank accounts – can be bought in lots of thousands or even millions, and buyers have the choices of 'raw' information or personal information that that has been tested for accuracy. These markets are one reason why cybercriminals are adaptive and dynamic in developing new tools and techniques that challenge cyber defenses.

The tools available for crime on the Dark Web continue to improve. Cybercrime attracts innovators and is a dynamic technological environment. There used to be a lag of somewhere between three and five years between the use of hacking tools developed by advanced intelligence agencies and their spread to cybercrime markets for purchase or rental, but this lag is shrinking. The evidence for this is anecdotal, but the trend has been consistent for several years. Recent events, such as the leak of advanced hacking tools on WikiLeaks or through the "Shadow Brokers," has accelerated the improvement in capabilities in both criminal groups as well as nations. Both of these recent leaks are probably the result of Russian intelligence activities, and the Russian state and cybercrime groups are deeply intertwined.

Russia is a haven for the most advanced cybercrime groups and no clear line delineates the criminal world from the government. The Kremlin sees Russian cybercriminals as a strategic asset, and one of the most difficult problems for reducing cybercrime is that Russia, along with North Korea, will not cooperate with Western law enforcement. High-end cybercriminal groups in Russia have hacking capabilities that are better than most nations. A Russian hacker was responsible for the Yahoo breach, compromising more than a billion credentials which were used

for both criminal and intelligence purposes. NoPetya was Russian malware designed to collect both intelligence and commercial information. Russian cyber criminals have likely hacked law firms, accountants, and investment companies to gain information that will let them manipulate financial markets.

The other state that supports cybercrime is North Korea (DPRK). North Korean government agencies have long used criminal activities to gain hard currency for the regime. The North has always relied on criminal activities - smuggling, counterfeiting, to gain hard currency, and in recent years, it has used the hacking skills of its principal intelligence agency, the North Korean Reconnaissance General Bureau (RGB), for cybercrime. The most famous examples of North Korean state cybercrime are the hack of the Bangladeshi Central Bank and Wannacry ransomware event.

These attacks provide a lucrative means to supplement the North Korean government's limited access to foreign currency and to evade sanctions. The DPRK uses variants of malware available on the cybercrime black market and has been successful mainly against poorly protected targets. North Korean cyber capabilities have not yet reached the level that would allow them to go after the most advanced targets (such as American banks), duplicate Stuxnet or the Russian attack on Ukrainian power facilities.

North Korea has also turned to cryptocurrency theft to help fund its regime. North Korean hackers have targeted at least three South Korean cryptocurrency exchanges in 2017.[2] Cryptocurrencies are a particularly valuable target for North Korea, who is able to use Bitcoin's anonymity to circumvent international sanctions. There is some speculation that North Korea has also installed bitcoin mining software on hacked computers to mine for cryptocurrencies. The Pyongyang University of Science and Technology now offers its students classes in bitcoin and blockchain.

Protected spaces on the dark web, an innovative cybercrime ecosystem, cryptocurrency and countries that engage in and support cybercrime – this is a daunting list of problems, but there are solutions. Each of these ideas deserves longer discussion, but in brief,

- The U.S. and its allies must develop an appropriate and effective strategy for punishing states that support cybercrime. This may need to go beyond traditional law enforcement activities to disrupt cybercriminal networks, software programs, and financial resources, much as the Navy had to take action against the Barbary Pirates. In general, the U.S. needs to develop retaliatory strategy, since as long as there are no penalties for malicious cyber action, our opponents see no reason to behave in cyberspace, and this applies to cybercriminals as well as states.

- Many countries are moving to regulate or even block cryptocurrencies. This is a draconian solution to the problem. Cryptocurrencies whose use can be done in ways consistent with anti-money laundering and other financial regulations should be allowed to operate. Those cryptocurrencies and related "mixing services" designed to evade

[2] Luke McNamara, "Why Is North Korea So Interested in Bitcoin?," FireEye, September 11, 2017

money laundering requirements should be banned.

- Widespread adoption of effective cybercrime laws by all countries remains essential, as countries with weak cybercrime laws tend to experience a higher rate of crime. The best vehicle at this time is the Budapest Convention.

- We are unlikely to ever be able to suppress the Dark Web, so efforts to disrupt and dismantle criminal networks should be expanded through increased resources and technology for law enforcement agencies and increased international cooperation.

- Expanded international law enforcement cooperation and the modernization of important tools like Mutual Legal Assistance Treaties (MLAT) are essential for countering cybercrime.

- Companies should ensure their cyber defenses are adequate. In the U.S. this has been done on a voluntary basis. Other countries are moving to a more regulatory approach that requires companies to meet higher standards of cybersecurity.

- Encryption remains a vexing problem. Opinion in many other countries is moving slowly toward greater constrains on the use of the kinds of encryption that create problems for law enforcement, but restrictions would face opposition from privacy groups in the U.S. and other countries. There is no consensus on possible solutions to the encryption problem. These solutions fall into two broad categories: restricting access to encryption that does not allow for recovery of plaintext by third parties or, alternatively, increasing law enforcement capabilities and resources to break encryption or use metadata to deal with the evidentiary problems encryption creates.

- Harmonization of international requirements for cybersecurity in important sectors like finance would both improve security and reduce the compliance burden on multinational companies.

- Finally, all nations would benefit from a serious effort at the national and international level to develop common definitions and measurements for cybercrime and collect data on its cost. We do this now for transnational crimes like narcotics or piracy, and cybercrime should be added to this list.

I thank the Committee for the opportunity to testify and welcome any questions.