BLURRED LINES: WHEN DOES CYBERCRIME BECOME AN ACT OF WAR?

High-profile data breaches are in the headlines almost daily. Federal law enforcement recently named cybercrime as its top priority, and numerous indictments of foreign nationals have been made under Title 18 of the U.S. Criminal Code for computer fraud, economic espionage, wire fraud, and money laundering. Theft of cash, trade secrets, and personally identifying information (PII) through the Internet is a constant risk. This session will explore the three key elements in profiling cybercrime.

You will learn how to:
- Define the stages and elements of the cybercrime process.
- Name the threats and victims.
- Identify the motivations, methods, and targeted assets of cybercrime.

DAVID SAWYER, CFE, CPA, CIA, CAMS
Partner and Practice Leader, Forensic and Special Matters
Frazier & Deeter LLC
Alpharetta, GA

David Sawyer leads Frazier & Deeter LLC’s Forensic and Special Matters practice. During his career as a forensic expert, he has investigated fraud, corruption, or financial damages in more than 200 cases. He has provided expert testimony in more than 20 of those matters. With his background as a practicing CPA, licensed private investigator, and internal auditor, he also consults with organizations on improvements of internal controls, as well as fraud prevention and detection. Currently, David is working as an advisor to the Cyber Economic unit of a global consulting firm on the initiative to combat, prevent, and detect multinational economic and military espionage, as well as the proliferation of WMD, terrorist financing, and money laundering.
Introduction
As use of the Internet has grown and as the computer and mobile devices have become more powerful, cybercrime has become a national and global criminal activity, reported almost daily. And this is not surprising, because cybercrime is perpetrated through the ubiquitous medium that affects every American—the Internet—and because, unlike most domestic criminal activity, it transcends international borders. Cybercrime not only poses a threat to individuals and businesses, but also our national security, because cybercrime and cyber-espionage undermine our domestic economy and defense. From the perspective of an investigator, the key to understanding cybercrime and other forms of cyber-attack is to ask and answer the fundamental questions of Who, What, When, Where, Why, and How / How Much.

Data Breaches in the Headlines
The list of victims in recent cybercrime breaches reads like a Who’s Who of government agencies and Fortune 500 companies. The list includes:

- Target
- Sony Pictures
- Home Depot
- T.J. Maxx / Marshalls / Homegoods
- Barnes & Noble
- JP Morgan Chase
- Anthem / Premera / Blue Cross
- Jimmy John’s
- The UPS Store
- United State Postal Service
- Dairy Queen
- Goodwill
- The National Weather Service
- Sally Beauty
- The White House
- Goodwill

The common ground shared by each of these organizations is that they possess an ASSET that is targeted with some
BLURRED LINES: WHEN DOES CYBERCRIME BECOME AN ACT OF WAR?

ACTION by a specified malicious ACTOR. The actors are driven by a particular ATTITUDE (i.e., motivation) and will follow a designated AVENUE, ACCESS, or APPROACH, depending on the situation or goal. Methods and motives may vary by industry or market AREA, as well.

Background
Expanded access to data, resources, and applications (can you say apps?) makes our lives more convenient. However, in order to gain this access, we must give something up, with that being certain aspects of our personal identifying information (PII) and therefore, some degree of our privacy. In doing so, we allow additional avenues for exposure or monitoring, to whomever might gain access to that information. Without proper security and controls, we become more exposed, whether we are individuals, businesses, or nation-states.

Avenues of access that might expose us include usage of the Internet, cell phones, and credit cards. Other avenues include satellite surveillance and closed-circuit television (CCTV) systems. It is estimated that more than 7 billion cell phones are in operation today, with most of them having the capability of being a tracking device. There are more than 5 billion active credit cards in use, with 1.5 billion being used in the United States alone. Internet usage can be tracked to follow our spending and buying habits, travel, associates, and behavioral patterns. Satellites and CCTV can monitor and follow our every movement.

Statistics
The FBI ranks cybercrime as the #1 threat to the United States, alongside terrorism. As the U.S. economy slowly recovers, financial and investment fraud schemes are on the rise, with many of them perpetrated via the Internet.
According to statistics, four in every ten emails contain some form of infection and the average period of detection for cybercrime is 229 days. The question is not IF or even WHEN you or someone you know will become a victim of cybercrime, but HOW LONG will it take to be discovered.

In 1984, there were 1,493 computers connected to what was then, the earliest form of the Internet. From 2000 to 2009, the number of estimated Internet users grew from 394 million to nearly 2 billion. In 2013, it was estimated that 39 percent of the world’s population had access to the Internet. Similar to Moore’s Law, the number of websites doubles every 18 to 24 months, which would equate to approximately 2 billion websites by 2015.

We are impressed (and appreciative) by how Google and other search engines can return millions of search results within seconds. However, the Deep Web—sites inaccessible to public-use search engines—is estimated to be 400–500 times larger than the indexed Web. Digital information is not like written information; it is changeable and susceptible to abuse. While the Deep Web is used predominantly for legal purposes, the Dark Web is most often used for illegal or illicit purposes. Examples of underground use of the Internet include TOR (The Onion Router) and Silk Road (taken down by FBI in 2013), which have been used for conducting transactions—often illegal—in virtual anonymity.

Pervasive as Internet use has become, especially with the proliferation of Web-enabled mobile devices and smart phones, the risk has also increased exponentially for cybercrime, cyber-terror, and even cyber-warfare. If they are not concerns already, they should be in the forefront of awareness for each and every user of the Internet.
Commercialization of Cybercrime

While malware is used to install viruses, worms, spyware, adware, and rootkits, crimeware packages, such as exploit kits and banking trojans, are designed expressly for use in cybercrime. Exploit kits that specialize in bank-account takeover or identity theft can be purchased—and the prices are declining to far less than $2,000 per “license”—so that the non-technical person can easily engage in cybercrime, with only minimal orientation or training. And cybercrime has become a thriving cottage industry. It seems that crimeware syndicates have adapted the business model of Silicon Valley and computer security firms (white-hat hackers). The purchased products even provide upgrades, customization, and technical support.

For example, it is estimated that the Zeus banking trojan has infected more than 3.6 million computers in the United States alone. In 2010, approximately 5,000 U.S. banking customers were robbed of more than $1.1 million. Estimates show that the programmers of this crimeware earn approximately $800,000 per year.

Much like drug cartels that evolved into sophisticated, multinational criminal business enterprises, cyber criminals employ networks of bulletproof hosting sites, proxy services, coders, SPAM services, exploit developers, crypting services, and cashing and money transfer services. Crimeware syndicates have copied the business model of Silicon Valley.

Sock puppets are Internet users’ alter-egos or aliases, designed to deceive genuine users. Astro turfing is the use of sock puppets by corporations in order to influence public opinion. As an extension to this method of social engineering, the same methods could be used to influence
public opinion regarding financial markets, political agendas, and the spread of propaganda.

*Sting boards* are false-front websites set up by law enforcement or security agencies to monitor and trap criminal activity. This application is used or might be used to combat cybercrime, cyber-jihad, or child pornography. *Honeypots* are computers placed on the Internet, with known vulnerabilities, with the intention of attracting hackers and observing the methods used to gain intrusion and exploitation.

*Phishing sites* play a part in sending tens of millions of phishing emails each day, containing a link to a counterfeit website, which closely resembles the website of the genuine company. Often, these sites mimic banking websites, requesting and recording PII credentials for later use and conversion.

With such vulnerability and exposure, the end result is a loss of trust (and perhaps paranoia?) by Internet users. A possible larger concern is the complete lack of awareness of these risks by the public at large.

**The Foundation: An Exploitation of Trust**

The entry point for a cyber-attacker—whether hacktivist, criminal, terrorist, or warrior— is the exploitation of a weakness or violation of trust. The cyber-attacker gains entry by using a trusted email address, website, software application, business relationship, internal network, or credential.

**High-Level Process Flow**

To segue into a more detailed discussion of cybercrime, let’s recap our basic questions, which we will call the Five W’s and an H: Who, What, When, Where, Why, and How /
How Much. With cybercrime—and really, most any fraud—the central premise is that there is an ASSET (What) targeted for the ACTION of theft or misappropriation (How). The ACTION is performed by a malicious ACTOR (Who) who is motivated by a certain ATTITUDE (Why). The ACTOR performs the ACTION upon an entity within a specific market or industry AREA (Where), using a prescribed APPROACH, ACCESS, or AVENUE (a combination of How, Where, and When). The ACTOR, whether an individual or a nation-state, might perpetrate this action internally (a trusted insider or employee of the victim firm), externally (unrelated to the firm), or in a partner capacity (a potential or actual party in a merger, acquisition or joint venture).

The Asset at Risk
The What is the ultimate Asset that is targeted for conversion by cyber-criminals or nation-state threat actors in order to achieve their intended objective or motive. These assets include, but are not limited to, cash, intellectual property and R&D assets, market and sales data, and reputation. Also at risk is personally identifying information (PII) such as name; address; date and place of birth; Social Security number; mother’s maiden name; and biometric, medical, educational, financial, and employment information. Each form of PII can be used for compromise or conversion of every aspect of a person’s worth and value, whether tangible or intangible.

Practical Application, by Market or Industry Area
Actors and Actions vary distinctly by industry Area. This is responsive to our investigative question of Where. For example, cybercriminals who are motivated by direct, individual financial gain have historically preyed on businesses in the banking, retail, and food-service industries. The targeted assets reside in bank accounts and
other monetary assets. By contrast, threat actors engaged in cyber-espionage have historically exploited intellectual property and research and development assets of defense contractors and manufacturing firms.

The prime targets for cyber-attacks, by industry with a few example risks, are listed below.

**Compromise of Personally Identifying Information (PII)**
- Finance and banking: account activity information
- Retail: credit and debit card numbers
- Health care: medical records and history

**Shutdown, Corruption, or Interruption of**
- Communications: telephone, cellular, satellite
- Transportation: traffic lights, rapid and mass transit
- Energy and nuclear power: shutdown or meltdown
- Water and sewer: drain excess runoff, water and sewage treatment
- National Weather Service: flaws and weaknesses in dam infrastructure

**Theft of Intellectual Property and Trade Secrets**
- Oil refineries and petro-chemical: explosions, chemical recipe for oil and gas mixture
- Aerospace: design plans for air defense weapons and aircraft
- Agriculture: crop science, including wheat, grain, corn, fruits, and vegetables

**Scenarios, Categorized By Attitude**
At the most general level, cyber-attacks can be categorized by the motivations or ATTITUDES behind the ACTION. The three macro-level categories are activities that are socially motivated (social), criminally motivated (criminal),
and nation-state motivated (nation-state). Anecdotally, the FBI model uses 27 different categories of cybercrime, with more than 60 subcategories.

Criminally motivated activities are driven by the desire for personal gain or business advantage. This threat vector includes economic espionage and gathering business intelligence or trade secrets to gain competitive business advantage.

Nation-state-motivated activities include cyber-terrorism or cyber-warfare, as well as military espionage and gathering military intelligence and information. As the lines blur, nation-state activity may well mask itself as organized (cyber) crime, such as bank fraud or economic espionage.

In general, the malicious activity is perpetrated via unauthorized access or exceeding authorized access to data or information and is prosecuted under U.S. Criminal Code, Title 18, Section 1030.

As we build our understanding of these motivating factors, we find that there is overlap, in that certain motives serve multiple purposes. For instance, the activity of terrorism financing—a close relative of money laundering—might not only involve criminal activity, but also be a threat to national security (warfare, terrorism, and espionage). The same dual-purpose intent could be attributed to the motivations for business advantage and shutdown or interruption, especially if perpetrated by an aggressor nation-state such as China, Russia, North Korea, or Iran.

The How: Approach, Avenue, and Access
Access, Approach and Avenue (How) are closely related and practically married at the hip to Attitude (Why) and market Area (Where). The method and conduit (ACCESS,
APPROACH, AVENUE) is often determined or driven by the motive (ATTITUDE) or industry sector (market AREA).

At its inception and foundation, cybercrime is initiated by some form of hacking or hacktivism. The method of attack most often includes hacking and the introduction of malware, by using the Avenue (Access point) of email or direct action (brute-force incursions) on the victim’s information technology infrastructure. Avenue also answers the How question, because it is the physical conduit—such as an individual computer, bank account or routing system, server, network, domain list, or human—that is used to gain access to the targeted asset. The Avenue is inherently less valuable than the targeted Asset(s), but is nonetheless a necessary evil to gain access to the more intrinsically valuable data.

**Attitude #1: Social Motivation**
Socially motivated methods, depending on the extremity, outcome, or intended results, may be legal or illegal. The Internet is construed as an extension to the First Amendment right to free speech and seen as the “fifth domain” of publicity. Postings on Facebook, YouTube, Twitter, and Instagram, to name a few, are legally used to promote an agenda, whether social, religious, idealistic, or political. The goal of cyber-social activism is most often social engineering or embarrassment. Within proper limits, this use of the Internet is legal. Cyber-activism uses the Internet in an effective way that does not break the law.

However, defacement of websites or false postings to social media websites may cross into the realm of illegality. There is a fine line between cyber-activists and cyber-hacktivists like Anonymous or LulzSec, where a person or group uses the exploitation of computer systems and networks to
advance their political or social causes. Numerous other illegal methods exist, such as phishing, spamming, cyber-stalking, and cyber-bullying. It is difficult to assign a financial damage amount to these activities.

The actions of distributed denial of service (DDoS), exploiting and compromising the flaws in publicly available software, and installation of malware (e.g., virus, keylogger, adware), while often socially motivated, may also be illegal. Installation of malware can result in the establishment of hijacked “zombie” computers, which can be used for illegal activities.

“Patriot hackers,” such as the Jester (th3j35t3r), use their skills to hack the perceived enemies of the United States. For instance, the Jester targets Internet websites that offer a platform for terrorists to spread propaganda, recruit new members, and offer online guides about how to construct improvised explosive devices (IEDs) and suicide vests. The Jester is reputed to have attacked WikiLeaks by using DDoS and assisted in the arrest of more than two dozen members of Anonymous.

**Attitude #2: Criminal Motivation**

As mentioned, hacking is the gateway to committing other types of cybercrime, which are motivated primarily by personal gain or business advantage. Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain.

Once-trusted insiders like Edward Snowden have stolen proprietary information for personal, financial, and ideological reasons. The cyber-criminal might be a former employee or a current employee who is disgruntled.
Methods in the hacking and cybercrime lifecycle include *intrusion*, where the victim computer is accessed with a compromised password. This access allows exploitation to occur by using *remote-access trojans (RATs)*, which take control of the victim computer and are capable of monitoring every movement and process on that computer. The victim computer is hijacked and turned into a *zombie*, part of a *botnet* of illegally hacked computers used by organized cybercrime syndicates. In this hostile takeover, the victim computer could be used to send spam, locate other computers for potential infection, or participate in DDoS attacks, while posing as the owner of the victim computer.

In general, the cyber-criminal will perform reconnaissance prior to the initial compromise of the system. Social media accounts have been known to be targeted and social engineering tactics have been employed. Malware is executed on the victim’s systems and a foothold is established. Once inside, the intruder can exfiltrate or destroy data. The intruder may then perform additional internal reconnaissance within the system. These internal lateral movements include expansion of presence and escalation of privileges.

In terms of modus operandi—or method of operation and perpetration—cybercrime is placed into three broad categories:

- Traditional crimes using the Internet as a medium (Internet-mediated crimes)
- Cybercrime with indirect costs
- Cybercrime with direct costs

*Internet-mediated crimes* include the sale of illegal or pharmaceutical drugs online, as well as online gambling, prostitution, or pornography.
**Indirect cost crimes** include spam, copyright violation, cyber-stalking, cyber-bullying, and pay-per-install schemes. Pay-per-install scams include adware, toolbars, or registry-optimization software that might be used to hijack the victim’s computer and launch malware or RATs. These are labeled as ‘indirect cost crimes’ because it is difficult to assign finite, concrete dollar value to the damage caused.

Some examples of **direct cost crimes** are:

- **Advance-fee fraud**, commonly known as a *419 Scam* or *Nigerian Scam* has existed practically since the invention of email (and even existed in the form of letters, prior to the existence of the Internet). The victim, out of greed and naiveté, sends money to the sender of the email to facilitate bank transfers that, of course, never occur.

- **Banking theft** is executed by using RATs, such as the Zeus Trojan. Malware is installed on a vulnerable victim computer, where bank account details are stolen by hostile takeover. Money is then stolen from available accounts or illicit funds transfers are made without the victim’s knowledge. Cyber-criminals then use “cash-out mules” to withdraw money from ATMs around the world in a single day. The cash-out mules usually earn a commission of 20 percent.

- **Business-opportunity schemes**, often referred to as work-from-home schemes or get-rich-quick schemes, offer the potential to earn thousands of dollars from the comfort of your own home, for a small upfront investment (franchise fee) at graduating prices for different levels of benefit or exposure (e.g., silver, gold, platinum). Of course, the return on investment never occurs. This category is similar to online-securities fraud or online-investment fraud.

- **Contacting clients to steal business** involves using contact lists (stolen from a current or former employer,
or even by an outsider) to contacts clients, perhaps offering lower prices that undercut the victim company.

- **Credit card fraud** is likely the foremost problem on the Internet. Blacklists are websites that sell stolen credit card numbers by the dozens. The stolen credit card number is used to make purchases; purchases of expensive goods are often returned for cash or sold at online auction sites such as eBay.

- In **cyber-commerce fraud** (often in the form of online auction fraud), the purchaser never receives the goods ordered or the seller never receives the cash. The intangible outgrowth is that confidence and trust decline in this form of conducting business.

- **Cyber-espionage** (or **spear phishing**) occurs when emails are sent to specific, strategic, high-ranking individuals within a company, containing a disguised link to a RAT. Once access is gained, the cyber-intruder might steal company secrets, new software under development, or other proprietary information for financial gain.

- **Cyber-extortion** is used to blackmail Internet users who have something incriminating to hide. The threat might also come in the guise of a threat from a governmental agency (e.g., FBI, IRS, utility company). The extortionist requests the payment of a fine, via credit card or wire transfer. A variation of this crime is when credit card numbers are stolen online and the victim is threatened that the card number will be published online unless a fee is paid.

- **Escrow fraud** involves a purchaser who deposits funds with a fraudulent escrow agent; the money is not returned or is used for the originally intended purpose.

- **Identity theft** involves stealing someone’s personally identifying information online to set up credit cards, take out loans, or obtain identity verification documents (driver’s license, etc.)
BLURRED LINES: WHEN DOES CYBERCRIME BECOME AN ACT OF WAR?

- *Payment solicitation by email*—posing as a legitimate, apparently familiar business, emails are addressed to business executives or high-net-worth individuals, requesting electronic funds transfers (EFT).
- *Phishing* is designed to entice the email recipient to access a counterfeit website (with the appearance of a bank, credit card company, eBay, or PayPal). The victim enters credentials, which are then used for credit card fraud or sold to be used for identity theft. In addition, the victims might have a botnet client or RAT installed on their computers.
- *Romance scams*—an online romantic relationship is established by an impersonator using a stolen photograph or image. Funds are often requested for various alleged personal crises, in order to facilitate an in-person meeting. The meeting, of course, never occurs.
- *Scareware and pay-per-install*—using the threat that a virus is located on the victim computer, or the promise of optimization or increased computer-processing speed, the victim pays between $50 and $129 for software that does nothing or is some form of malware.
- *Social network fraud*—an email comes from a contact in your email address book or online social network. The message from the email account, which has been compromised or hijacked, states that the “friend is in trouble” while traveling in foreign country. Scenarios include a stolen passport, stolen money, medical problems, or false imprisonment. The fraudulent email requests money via electronic transfer to make bail, fly home, etc.

**Attitude #3: Nation-State Motivation**

So when is the line crossed, from criminal activity and motivation to activities such as warfare or terrorism that are driven by the agendas of nation-states or ideologies that
BLURRED LINES: WHEN DOES CYBERCRIME BECOME AN ACT OF WAR?

might not be inherently criminal? Many times, these activities mimic each other or serve multiple different malicious purposes.

Generally, nation-state actors use *espionage* to conduct computer intrusions to steal sensitive state secrets and proprietary information from private companies. *Terrorism* groups might sabotage the computer systems that operate our critical infrastructure, such as utilities grids. In *cyber warfare*, nation-state actors sabotage military and critical infrastructure systems to gain an advantage in the event of a conflict.

### Cyber-Espionage and Intelligence

Military cyber-espionage includes the theft of military or national security secrets, as well as intellectual property, including designs for weapons and defense systems. In addition to cyber-attacks inflicting disruption or destruction of data and infrastructure (sabotage), other traditional Cold War–spy methods and covert warfare approaches have a cyber-application, too, including espionage, surveillance, and infiltration. The Internet has multiplied the impact of these activities exponentially. Cyberspace is an ideal arena for psychological warfare (PSYOPS), in that public and political opinions can be influenced on a mass scale through the social media.

### Cyber-Terrorism

Terrorism is the use of violence or the threat of violence to cause fear, panic, and demoralization of a community, in pursuit of a political or religious goal. General categories of terrorism include right wing, left wing, nationalist, Palestinian, and militant Islamist or jihadi.
While right-wing terrorism intends to replace the state with a dictatorship of the mind, left-wing terrorism’s objective is to replace the current “bourgeois capitalist hegemony” with a society that is arranged according to the ideology of a more socialistic or communistic Marxist-Leninism philosophy.

Nationalist terrorists see themselves as freedom fighters with the goal of overthrowing current government or liberating their country from perceived colonialist oppression.

Palestinian terrorists regard the Israeli government as an occupying force in their homeland. These groups include Fatah, Hezbollah, and Hamas.

Militant Islamist or jihadi terrorists, including Al-Qaeda and ISIS / ISIL, use the Internet for many purposes, such as distribution of propaganda materials against their perceived enemy; homemade videos of attacks; and training materials for operations, weapons, and bomb-making. They also use the Internet for distribution of counterintelligence materials, such as law-enforcement techniques and intelligence operations and online forums for communication.

Modern terrorists use the Internet as a weapon to train the next terrorists and spread their message of insurgency. The use of cybercrime techniques to raise funds for terrorist operations and provide long-range logistical support to active terrorist operations further blurs the line between cybercrime and cyber-terrorism.

Cyber-Warfare
The tactics, techniques, and procedures (TTP) used by cyber-warriors are similar, if not identical, to those used...
BLURRED LINES: WHEN DOES CYBERCRIME BECOME AN ACT OF WAR?

by hacktivists, cyber-criminals, and cyber-terrorists. However, the differentiating factor is the underlying motivation for the attack.

U.S. military doctrine is to dominate the battle space whether it is on land, at sea, in the air, in space, or in cyberspace. According to former Presidential cyber security adviser Richard Clarke, cyber-warfare can be defined as “actions by a nation-state to penetrate another nation’s computers or networks for the purpose of causing damage or destruction.”

The first objective of cyberwar is to degrade information, to the point that it cannot function and cannot be trusted. Other objectives include injecting disinformation and attacking vital infrastructure, such as nuclear reactors, pumping stations, dams, and power plants.

Cyber-warfare is an extension of normal, conventional warfare. It is sanctioned by a nation-state and dictated by foreign policy, in terms of defining acts and responses. Cyber-warfare has become integrated into the normal functions of traditional covert warfare, espionage, and black operations. Research and development of cyber-weapons is well underway, along with a presumed cyber-arms race. Cyber-war games that simulate attacks and conflicts are also waged within U.S. military branches (Army, Navy, Air Force, and Coast Guard).

Cyber-war has attributes that make it appealing on several different levels. The most obvious factor is the low cost. Web infrastructure, developers, and black-hat operators are already in place. Risk and visibility are also low, because detection of actors is challenging and
time consuming. It is becoming easier to fly under a false flag. Further, the supply of *mercenaries* or *proxy warriors* is abundant and, therefore, less costly. Another contributing factor is the relative ease and convenience of *plausible deniability*.

**Actors for All Motivations**

The ACTORS (Who) can be individuals and nation-states alike. There is a striking correlation between the country from which threat actions originate and the motive or type of action. Cybercriminals based in the United States, Russia, and Eastern Europe (e.g., Romania and Bulgaria) have historically focused on financial crime, while actors in China have engaged in economic espionage.

*Level-one actors* include the United States, Russia, and China. These nation-states are more technologically advanced, with a large population of potential hackers. Related to existing conventional military might, these nations hold the highest level of cyber-warfare capabilities.

*Level-two actors* include Pakistan, India, North Korea, and South Korea and can be aligned with one or more level-one nation-state actors. These nations seek formal or informal partnerships with larger, higher-impact players, by sharing and developing technology together.

*Level-three actors* include the United Kingdom, France, Iran, and others. To be more autonomous and competitive with level-one and level-two actors, substantial investment in cyber-warfare or direct purchase of a cyber-weapon is necessary.

While minor skirmishes can be seen between these various nation-state actors, it is becoming increasingly clear that an arms race is heating up on the cyber-front.
Military and Federal Law Enforcement Response and Action
The definition of *enemies*, both foreign and domestic, can be viewed in a different light with the emerging threat of cyber-attacks. The United States seeks to protect its interests by gathering and analyzing intelligence, both in human form (HUMINT) and electronic or signal form (SIGINT). This effort has been demonstrated in electronic monitoring programs such as Echelon, Mainway, Marina, Nucleon, and Prism.

As seen in recent indictments of cyber-criminals who are foreign nationals, U.S. law enforcement is taking an aggressive posture toward cybercrime, as well as activities that might evolve into cyber-warfare. Ongoing sanctions continue against nation-states that are labeled as *jurisdictions of proliferation concern* or shelters for terror organizations.

Below is a list of workhorse statutes that have been used for federal indictments of cyber-criminals. These indictments have resulted in the compilation of the FBI’s Cyber Most Wanted List. Under Title 18 of the U.S. Criminal Code, the sections below have been utilized for federal investigation and indictment of cyber-criminals.

Computer Fraud (Section 1030) as a conduit or hub statute for:
- Economic Espionage (Sections 1831–1839)
- Racketeering (Sections 1961–1968)
- Identity Theft (Section 1028)
- Wire Fraud (Section 1343)
- Bank Fraud (Section 1344)
- Money Laundering (Sections 1956–1957)
- Securities Fraud (Section 1348)
CONCEPTS OF COUNTERMEASURES

Rumors abound that new initiatives are underway that will create an individual profile for every person on earth, tracking their Internet usage, phone calls, credit records, posted photographs, buying habits, and purchases. While helpful in tracking criminals, terrorists, and enemies of a nation-state, the concern is that innocent people will become victims if the system is abused, misused, our hijacked. In today’s cyber-world, even going off the grid might not be a solution and appear as suspicious.

With the growing capability of data warehousing and powerful search engines and scripts, the same means and methods that make us vulnerable might also be the tools that help us apprehend cyber criminals, terrorists, and warriors. Monitoring wire transfers and certain credit card activity might indicate certain unlawful behaviors. Even several degrees of separation with a social networking contact can link two people and serve as a puzzle piece during an investigation or intelligence operation. Patterns of search-engine activity might indicate interests and motives. Shared links and postings with certain content might be illegal in certain countries, because it might provide information that is harmful to the general public or aid criminal or terrorist endeavors. If cell-phone movement or tracking appears irregular, it might indicate that an attempt is being made to use cellular technology that obscures location information. Data from airlines, rail systems, shipping lines, or hotel records can indicate travel to jurisdictions where certain criminal or terroristic activities are ongoing or sheltered. Using Internet café’s in certain geographic areas, at certain timeframes or increments, can be indicators of suspicious activity, to reveal (or fill in) gaps of a specific person’s whereabouts and communication. Even individual computer filenames or types can indicate suspicious activity. When compared
to the names of certain individuals on no-fly lists, the collective impact of this information can become a useful, powerful tool in combating cybercrime and cyber-terror, as well as waging cyber-warfare or intelligence operations.

**Prevention: What Can We Do?**

As individuals, there are basic ways we can avoid or prevent exploitation. Using and installing updated software is a good first step. Software and operating systems are often updated or patched because weaknesses are found that make the programs more vulnerable to hacking or malware infection. Using firewall protection and anti-malware programs (anti-virus, anti-spyware, anti-botnet, etc.) can also prevent unauthorized intrusions to your system.

At the corporate level, the CIA principle is foundational”: businesses should ensure the confidentiality, integrity, and accessibility (CIA) of their systems and data. Password-protected systems are essential for confidentiality. Many, if not most, data problems can be prevented or mitigated if systems maintain integrity, by being consistently programmed and complete. Backups and redundancy servers are ways to ensure that data is preserved and accessible.

In his book *Cyber Attack*, Paul Day lists these six proactive measures:

1. Interfere with distribution of crimeware via filtering, automated patching, and countermeasures against content injection.
2. Prevent infection of computing platform with protected applications.
3. Prevent the crimeware from executing by validating code.
<table>
<thead>
<tr>
<th><strong>BLURRED LINES: WHEN DOES CYBERCRIME BECOME AN ACT OF WAR?</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>4. Prevent the removal of confidential data by restricting access to it with unauthorized code at hardware level.</td>
</tr>
<tr>
<td>5. Prevent the user from providing confidential information by monitoring keystrokes or providing a hardware-level trusted path.</td>
</tr>
<tr>
<td>6. Interfere with the ability of the attacker to receive and use confidential data by encoding data in a form that renders it valueless to attacker.</td>
</tr>
</tbody>
</table>

Collectively and conceptually—both at the individual, business, law enforcement, and military level—we all must work together to combat cyber-attacks. First, we can DENY cyber-criminals access to our computers. Second, we must DISRUPT and DEGRADE the support network used by cyber-criminals and slow their attacks on other victims. Finally, the ultimate goal is to remove the threat, or DISMANTLE and DESTROY the domestic and international networks that proliferate cybercrime and the nation-state actors that allow it or enable it to flourish.