CHAPTER 5

Know Your Enemy

5.1 HACKERS

5.1.1 They Don't Wear Balaclavas

The people who carry out cyber attacks are largely anonymous figures – famously caricatured in thousands of media stock photos as faceless youths in hoodies, wearing 'Anonymous' Guido Fawkes masks or balaclavas, and typing fiendishly at computer keyboards in black burglars' gloves.

The reality is that cyber hacking has progressed from its early stereotype as a hobby for amateur teenagers in their bedrooms to a professionalized, informal but well-organized, international industry with a hierarchy of participants, a set of guilds with niche specializations, its own social networks, cryptocurrencies, trading networks, e-commerce markets, communication systems, and vocabulary. Cyber attackers are commonly referred to as 'threat actors' (by theoreticians), 'hackers' (by us), 'black hats' (by the security community), 'the red team' (by company IT staff), 'perpetrators' (by the law enforcement community), and the 'bad guys' (by everyone else). Cyber attacks are criminal acts, so it is also correct to call them 'cyber criminals'. In general we prefer the term 'hackers', with no disrespect to the many ethical hackers who work on the side of the angels, and are sometimes called 'white hats' or 'the blue team'. We will generally mean criminals when we refer to hackers.

In addition to the threat of external attack, businesses and organizations are vulnerable to cyber compromise from their own employees and internal trustees. Many cyber attacks have occurred from disgruntled insiders, whistle-blowers, rogue traders, and internal saboteurs.

Although hidden and criminalized, the cyber black market behaves like most other sectors of the economy, subject to supply and demand, conscious of cost structures and cash flow, and requiring capital that needs to produce a return on investment. It operates using global and dynamically reconfigurable infrastructure that defies the geographical jurisdictional constraints of conventional law enforcement. The costs, rewards, and business models of hackers are known as hackonomics. We outline here how the understanding of hackonomics helps with devising security strategies and protection measures to reduce cyber risk.

Many companies go through red teaming exercises where they role-play how they would mount a cyber attack on the company, and have to imagine the motivations and priorities of the protagonists they will face in real life. The defending team is usually referred to as the blue team. Let's meet the teams.

5.1.2 In the Red Corner ...

It is useful to know what we are up against when we are trying to solve cyber risk. Cyber risk is more than cyber security systems and technological superiority. It is about understanding the motivations, the capabilities, and the 'tactics, techniques, procedures' (TTPs) and targets of the protagonists. Hackers are not a homogeneous bunch. We segment the universe of hackers into the following seven types, described further in the next sections:[1]

1. Amateur hackers
2. Hub-structured cyber criminal gangs
3. Hierarchically organized cyber criminal syndicates
4. Mercenary teams
5. Hacktivists
6. Cyber terrorists
7. Nation-state and state-sponsored cyber teams

Although all cyber criminals try hard to be anonymous and undiscovered, we know quite a bit about the activities, motivations, and capabilities of them as groups, even if we may not know their names or exact information. We can piece together profiles about them from the individuals who are arrested by the law enforcement teams, and from the information about the attacks they perpetrate and the fingerprints they leave behind them. We may not have enough evidence to convict in a court of law, but security specialists work on a principle of 'soft attribution': assigning the perpetrator on the balance of probability of the evidence.

There is an increasing interest in cyber criminology, becoming an established discipline of social science, research, and publication, with teaching courses being offered at universities, academic journals, and conferences providing a body of published studies.

5.2 TAXONOMY OF THREAT ACTORS

5.2.1 Amateur Hackers

Amateur hackers are people who do not earn their living from hacking but have a passion for working with computers, a curiosity for what they can achieve, and a flexible attitude to right and wrong. They are often experimenting or part of a community or social group, alerted to techniques and computer tools they can use through the forums and chat channels they share. They are commonly disparaged as 'script kiddies' (or 'skiddies'): people who use someone else's script or code to hack into computers, as this is easier or they don't have the skills to write their own.

Amateur hackers are individuals who have curiosity and some base levels of skills, and can occasionally pull off some surprising accomplishments by penetrating previously unknown vulnerabilities. As cyber attack tools

AMATEUR THREAT ACTORS

Teenage Hackers (and Not So Teenage)

Some of the headlines about cyber crime have been made by the young age of amateur hackers who achieve notoriety, such as Jonathan James, alias '*cOmrade*', who was arrested at the age of 15 for hacking into the US Department of Defense. James went on to be suspected of several other cyber crimes, suffering house arrest, serving jail time as the youngest person to be convicted of violating cyber crime laws, and finally shooting himself while under investigation for a major hack of protected customer data from TJX in 2007.[2]

Youth is a common characteristic of the experimental amateur hackers. A 14-year-old (too young to be named in court) exemplary pupil at his school, who had achieved outstanding grades in electronics, adapted a television remote control to change the points in the tram tracks in his hometown of Lodz in Poland, causing a tram to derail and injure 15 people.[3]

But not all amateur hackers are young. '*Astra*' has never been publicly identified other than as a 58-year-old Greek mathematician working alone and in his spare time, who was arrested for hacking into the Dassault Group and stealing weapons technology information to sell on the black market.[4] His hacking cost Dassault $360 million in damages.

become increasingly commoditized, there is potential for people with relatively low levels of skill and capability to deploy toolkits that have been developed by others and to apply them with increasingly damaging effect. As they graduate from script kiddies to becoming kit kiddies, they become increasingly powerful. The amateur hacker can also graduate by going pro. The pool of amateur hackers acts as the feeder system for the various layers of more sophisticated threat groups.

5.2.2 Hub-Structured Cyber Criminal Gangs

An example of an amateur going pro, Albert Gonzalez began as teenage hacker, and graduated to organizing his own international organized cyber crime gang. He was known as *soupnazi* at his South Miami high school, where he enjoyed and played up to his reputation as a computer nerd, becoming notorious at the age of 14 for hacking into NASA networks. He gathered other computer programming enthusiasts into his orbit and by the age of 19, having moved to New Jersey, he helped organize a group calling itself the *ShadowCrew*.

Hub-structured cyber criminal groups are thought to be the most numerous and active in the organized cyber crime economy. They are amorphous and each group may not last long before re-forming as another team. Some estimates put the number of active hub teams at around 6,400, suggesting that more than 100,000 individuals might be active in this sector of the cyber black economy,[5] but everyone acknowledges that it is difficult to quantify. The core gang members maintain a loose affiliation with a wide range of individuals, including specialists in exploit development, botnets, malware, phishing, ransomware, social engineering, and the monetization process of cyber crime. Each hub may have tens of core gang members, and the peripheral criminal fraternity that trades with this core, both providing services to them and buying their outputs from them, may number several thousands.

Unlike other criminal sectors of society, the members of this community are not the disadvantaged, poorly educated, marginalized individuals who constitute the bulk of traditional criminal activity and convictions. The typical profile of individuals convicted related to hub-structured cyber criminal activity is ‘aged 14–30, middle class, with high levels of educational achievement, predominantly white’.[6] Geographically, the known and suspected perpetrators are from regions with high levels of graduate unemployment, although not all regions with high levels of graduate unemployment give rise to populations of hub cyber hackers.

HUB-STRUCTURED CYBER CRIMINAL GANGS

ShadowCrew Cyber Criminal Gang

The *ShadowCrew* group that Albert Gonzalez pulled together from his computer nerd friends had around 20 core members, and was organized to steal credit card credentials, ATM codes, and other stolen identity data, such as Social Security cards, health insurance, and passport information. They set up and ran an auction website for stolen data, which attracted a loose affiliation of around 4000 individuals who bought and sold stolen information. In total they stole data that made them an estimated $4.3 million. They mounted some sizeable hacks of companies to steal protected data, including hacking 5000 credit card credentials from Dave & Buster's corporate network in 2007, and an alleged theft of 45.6 million credit and debit cards from TJX from 2005 to 2007.[7]

The *ShadowCrew* group shared its technology and methods with other related gangs of cyber criminals, including *Carderplanet*, a Ukrainian and Russian group of cyber criminals, and *Darkprofits*, a black market online trading site offering a range of stolen goods. Unlike legitimate businesses that compete with each other, these organizations cooperate with each other and share goods, services, and members in an informal network. Individuals in one group would also work with another, and associates with specialties are shared and recommended across from one team to another. This type of clustering of cyber criminal activity around core teams with leading members and a peripheral set of associate members is classified as 'hub' cyber crime.[8]

Albert Gonzalez's hub of activities spread to groups in a dozen countries in North America, Eastern Europe, Scandinavia, and Western Europe. He was finally arrested following an extensive Secret Service investigation (*Operation FireWall*) and agreed to cooperate with the authorities and provide evidence, which enabled the indictment of at least another 30 individuals, among them several key individuals who the authorities identified as being hubs of key cyber crime organizations in the United States, Turkey, and Russia.

It is estimated that up to 80% of cyber crime is committed by groups with some form of organized activity, either hub-structured or hierarchical.[9]

5.2.3 Hierarchically-Organized Cyber Criminal Syndicates

A separate and distinct pattern of organized cyber criminal activity is hierarchical organizations of teams that include hackers.[10] These organizations have formed from traditional organized crime, moving to add cyber crime to their activities, as well as some cyber criminals developing start-up hierarchical structures that mimic organized crime practices but that specialize in cyber activity (sort of 'disruptive' new start-ups to compete with complacent old-crime business models, to use an analogy from the legitimate digital economy).

Hierarchical cyber groups are similar to traditional criminal organizations, with a clear management structure, division of labor, and accretion of proceeds towards the top of the control pyramid. Traditional crime groups have embraced cyber crime as a new vector of profit. Europol estimates that it is dealing with 5000 international criminal organizations operating in the European Union, with a significant number of those operating to some degree in the cyber black economy. It is likely that blocs of similar levels of organized crime exist in North America and in other major regions of the advanced economies.

These hierarchically-organized cyber criminal groups operate with structures that are similar to traditional organized crime, and with characteristics that would not look out of place in any business in the 'white' economy. They have management structures to control expenditure (albeit enforced a bit more brutally than you might find in conventional businesses), track profitability, identify opportunities, invest in research and development, and optimize their return on investment.

Many of these groups invest in physical assets, buying property to house their operations in, and investing in high specifications of IT infrastructure and equipment, and other costs related to running a physical business. There has been evidence of hierarchical organized cyber crime groups having a marketing department, 24/7 customer care lines, ransomware call centers, executive benefit packages, and even a human resources department (maybe even criminals can't get away from performance reviews?). To protect these fixed assets from interdiction by law enforcement, these have to be located in safe areas outside their jurisdiction. Countries with poor law enforcement, with weak extradition laws, or without international cooperation agreements, are favored locations. This has given rise to widely publicized enclaves in countries like Romania: the town of Râmnicu Vâlcea (AKA 'Hackerville') in the foothills of the Transylvanian Alps has become notorious for its population of Mercedes-driving unemployed computer science graduates, and its concentration of IP addresses suspected of being origin points of dubious transactions.[11] Interpol is reported to be investigating criminal extra-jurisdictional hacker centers in many different countries, including Armenia, Azerbaijan, Brazil, Indonesia, Mexico, the Philippines, Russia, Taiwan, Turkey, and Vietnam.[12]

Hierarchical cyber crime groups have more stability than hub-organized crime groups, which enables them to invest capital in their equipment and teams, and so can build up expertise and capability. Some groups have shown a willingness to invest time and money in patient preparation for an attack, developing software and customizing tools for a specific target. They also reinvest some of their profits after a successful operation to improve their abilities and generate more money from their next attacks.

Despite the scale of their robberies, software experts suggest that the *Carbanak* team are far from being the most skillful software engineers. They have typically assembled toolkits and compiled software from multiple sources, repurposing the malware they create from a library of sources, and subcontracting key components of their systems from mercenary coders.

It is clear, however, that the *Carbanak* team and other hierarchically organized syndicates are much more than producers of software. They are business enterprises, albeit operating in a black economy. They have dedicated teams to research and identify their targets, specifically looking for hooks for their spear phishing campaigns. These employ social engineering techniques to find tricks that are most likely to fool a senior executive or an accounting clerk to click on the link in the email that will download the malware into the corporate network. They also invest in building sophisticated money-laundering operations.

These syndicates are motived to maximize their economic profit by choosing targets and attack vectors with the lowest cost. They invest in targeting, but they also operate opportunistically. They maintain lists of the types of companies they would like to gain access to, but also operate 'watering holes' operations where they will set out bogus websites or activities that could attract the kinds of individuals that they are interested in, and will wait to see if they get a bite.

Although there is a lot of variation between different syndicate operations, hierarchically-organized syndicates are generally considered to be more of a threat than hub-structured cyber crime gangs, as they concentrate capital, invest in new crime enterprises, and have greater resources at their disposal.

HIERARCHICALLY-ORGANIZED CYBER CRIMINAL SYNDICATES

Carbanak Cyber Crime Syndicate

Carbanak is a cyber crime syndicate, also known by security analysts as *Fin7*.[13] This group specializes in cyber attacks to steal credit card credentials and financial information that can be used fraudulently to steal money. They have targeted banking, retail, hospitality, and other business sectors. Their attacks have followed a similar process of tactics, techniques, and procedures (TTPs) that investigators have dissected after each of their operations. Most significantly, the group has evolved remote access Trojan (RAT) software that can penetrate a company's defenses and then operate from within their network, each evolution of their software remaining undetected from scanners that have been trained to look for the indicators of compromise published by security analysts who have studied their previous versions. In 2016, the group went on to develop an even more powerful generation of malware, based on the *Cobalt Strike* penetration testing software. *Carbanak*'s name comes from two of their early Trojans, *Carberp* and *Anunak*, used to break into banking networks.

A typical *Carbanak* operation involves handcrafting an entry into a target company, typically involving spear phishing, followed by a rapid scanning of the network to find financial transaction systems, point-of-sales systems, ATM networks, and databases of credentials information. Once they have found these data vaults, they escalate their privilege credentials to gain control of the systems, de-encrypt databases, and begin bulk harvesting and exfiltrating the information in well-disguised data streams. Stolen credit card data is efficiently sold on quickly through carder forums. ATM machines are reprogrammed to spit out cash at prescheduled times ('jackpotting'). One of *Carbanak*'s trademarks is the speed at which they operate once they have gained access.

Carbanak-like fingerprints have been found at the scene of more than 250 major financial data exfiltration attacks. One of their most notorious campaigns was against financial institutions in Russia, the United States, Germany, China, and Ukraine lasting at least a year from 2013, siphoning money into laundering accounts through the SWIFT banking system, extracting money through ATMs, and selling on stolen credit card details. Exact details of all the losses have never been made public, but one bank reported a loss of $10 million, and another had $7.3 million stolen from its ATM machines.

Some estimates suggest that *Carbanak* may have got away with as much as a billion dollars.

An international hunt by law enforcement agencies resulted in the Europol arrest in Spain of the leader of *Carbanak* in March 2018.[14]

5.2.4 Mercenary Teams

Mercenary teams of software coders and specialists of various types now offer their services on the cyber black markets. These services cover a wide array of tools and techniques, including offering 'for-rent' botnets,

MERCENARY TEAMS

Hidden Lynx Hacker-for-hire Operation

Hidden Lynx is a professional hacker-for-hire operation, based in China, that is contracted by clients to provide information, including industrial secrets and protected data. The group is named after a text string that was observed in their command-and-control server communications.[15]

They steal on demand whatever their clients are interested in, and tackle a wide variety of missions and targets. The group has carried out at least six significant campaigns since 2011. Their ability to mount multiple international campaigns at the same time with high proficiency using different tools and techniques suggests that they have considerable hacking expertise at their disposal, estimated at between 50 and 100 operatives, organized into a number of teams.

They have hit hundreds of organizations worldwide, with widely varying characteristics, including financial, educational, and government sectors, and many of their targets have been in the defense industrial sector of Western countries.

They have gained a reputation of being experts in being able to breach well-protected networks, and have two particular playbooks: mass exploitation using a specially designed Trojan, and pay-to-order targeted attacks, including a zero day implementation, to obtain intellectual property. They have broken into some of the best-protected organizations in the world and are considered one of the most capable independent cyber threat teams outside of nation-state control.

designing malware, trading zero day exploits, and providing professional hackers-for-hire to attack organizations.

Mercenary groups usually consist of small teams of skilled and experienced developers who are hired by organized cyber criminal groups to hack targets or develop malware or exploits that may be beyond the skill level of the personnel of most organized cyber criminal groups. They require sophisticated technology and infrastructure to operate, so skilled individuals who may have no particular criminal alignment originally have joined these mercenary teams to monetize their skills on the black market, within a team that offers specialized challenges and sells these skills through a black market to the highest bidder.

5.2.5 Hacktivists

Ideologically motivated cyber attacks have become an increasing threat in the cyber black economy. Hacktivist cyber groups typically represent counterculture or protest movements, and may be offshoots from or aligned with political and social organizations.

Information-age protests include defacing websites, spreading propaganda, providing or combating fake news, organizing hate mail and trolling campaigns, DDoS attacks, and network breaches against targets. They have also escalated into more damaging threats, such as bringing down the internet, to protest global inequality. Hacktivist movements have included anti-capitalism, anarchist anti-government, anti-military, and anti-copyright laws movements; radical ecological movements; political movements such as pro-Palestinian protests; and human rights, animal rights, anti-pornography, anti-terrorism, and other causes.

Hacktivist groups like *Anonymous* tend to operate in a ‘swarm’, as a large collective movement bound by a common purpose but with no clear leadership and with a minimal command structure. The capability they can bring to bear against their targets depends on the skills of the individuals who are motivated to contribute, and this may depend on the passion generated by the specific cause.

Other hacktivist organizations may be more focused and have a central organization and operational team that have caused damaging cyber attacks on businesses and government organizations that parallel activism, and damaging physical attacks on employees and property.

Hacktivists also encourage whistle-blowing, where insider employees of organizations release confidential information that shows up their employers

HACKTIVISTS

Anonymous

Anonymous is an international hacktivist group that has carried out direct-action protest campaigns of cyber attacks against authoritarian government, big business, and other targets, such as the Church of Scientology. Campaigns have consisted of distributed denial of service (DDoS) attacks on websites and servers, data breaches, causing localized internet outages and interrupting communications, distributing malware, spoofing control systems, and defacing websites. It also embraces a lighter side of a counterculture approach to in-jokes, pranks, and computer obsessions.

Anonymous has no formal membership but uses social media to coordinate and derive consensus for action, and crowdsources volunteers to act on suggestions. It embraces a distinctive brand and encourages its members to remain anonymous, popularizing stylized Guy Fawkes masks.

An *Anonymous* attack on Sony in 2011 compromised 77 million PlayStation Network accounts, causing the company significant commercial loss.

Anonymous and similar hacktivist groups took an interest in the 2011 Arab Spring uprising, helping dissidents in Arab countries access government-censored information and attack official websites.

They continued their support for populist uprisings when they helped coordinate the Occupy movement (Occupy Wall Street, Occupy London, etc.) later in 2011, when anti-austerity resentment combined with protests against social and political inequality and instances of corporate malfeasance, under the slogan ‘We are the 99%’, brought millions of people onto the streets of 950 cities. This was accompanied by ‘Operation Global Blackout’ – a threat that failed to materialize to cripple global business by sabotaging the internet using a specially-created cannon to carry out a DDoS attack on the root Domain Name System (DNS) servers.[16]

Over the years *Anonymous* has been associated with many campaigns against people and organizations they take issue with. The capability of the group to muster a coherent threat of high capability depends on the collective will and skills of the volunteers who care about the specific issue.

or sheds light on malpractice. One of the most notorious data breaches, the Panama Papers, saw an insider release 11 million confidential tax documents from a commercial law firm, Mossack Finseca, in 2016, to highlight 'income inequality' by disclosing how high-profile individuals hide income and avoid paying taxes.[17] Sites such as WikiLeaks, offering an outlet for the publication of leaked information, have become synonymous with hacktivism.

5.2.6 Cyber Terrorists

Terrorist groups seek political change through violence. Terrorism has a long history, with many sudden changes in tactics, as underground terrorist groups seek the element of surprise against the more powerful resources of law enforcement and the established political order.

Terrorist groups commonly use information technology to assist their cause, ranging from spreading propaganda and recruitment, to enabling encrypted communications between members, through to information gathering on counter-terrorism operations against them, raising funds through cyber crime, and providing operational support to physical attacks.[18] A specific convergence of hacking and terrorism is the publication of 'kill lists' of stolen data on military personnel to urge followers to attack them.

Many commentators have speculated on the future next phase of terrorism, ranging from terrorist groups acquiring various types of weapons of mass destruction, through to all-out economic and psychological warfare, or repeated use of insurgency tactics undermining the political tolerance of Western populations. A common area of speculation is that terrorists may seek to carry out spectacular destructive and mass-casualty attacks using cyber hacking techniques.[19]

The US State Department lists 58 organizations as foreign terrorist organizations. Many other Western countries maintain similar watch lists of proscribed international terrorist groups. Terrorist groups range from right-wing survivalists to separatist political movements, extremists of several religions, and groups espousing violence to support specific issues. In the twenty-first century, the leading, but not the only, terrorism threat to Western democracies has become the militant Islamic movements of groups such as Al Qaeda and the Islamic State (IS). The militant Islamic movement has generated cyber divisions, such as *Al Qaeda Electronic*, *United Cyber Caliphate*, *Cyber Caliphate Army*, *Afaaq Electronic Foundation*, *Syrian Electronic Army*, *Hezbollah Cyber Group*, and others.

CYBER TERRORISTS

United Cyber Caliphate

United Cyber Caliphate, also known as *Islamic State Hacking Division* and *CyberCaliphate*, is a disparate group promoting itself as the digital army for Islamic State of Iraq and Levant, effectively the cyber team of the Islamic State terrorist group. It carries out cyber attacks, such as the defacing of websites, the hacking of emails, credit card theft for fund raising, and data exfiltration attacks, for example to post 'kill lists' of the names and addresses of serving Western military personnel to exort followers to attack them physically.

The *CyberCaliphate* is a disparate group of volunteer followers of the violent ideology of the Islamic State, a militant Islamic group. The IS membership is responsible for terrorist acts such as bombings, mass killings, and attacks on military forces in Iraq and Syria. It has claimed responsibility for murderous attacks in Western countries.

The main activities of *CyberCaliphate* are predominantly propaganda and IT support to their cause, posting messages to followers and spreading the ideology to gain volunteer recruits; facilitating communications and enabling encrypted messaging between members to avoid detection; and information gathering, listening, and data gathering on anti-terrorist operations against them.

Originally the leaders of *CyberCaliphate* operated servers and computer networks from buildings located in towns in Iraq and Syria controlled by IS in their self-proclaimed caliphate, but these were consistently located by US and Western alliance military, and targeted and frequently destroyed by drone missile attacks from 2014 to 2017. Several of the known key figures in the *CyberCaliphate* were killed in targeted strikes.

Following the recapture of the geographical territory held by IS in Iraq and Syria by the combined military efforts of Western, Russian, and local forces, IS members have largely dispersed, with many of the foreign volunteers who were fighting for IS returning to their home countries. Abu Bakr al-Baghdadi, the leader of IS, has urged its membership to continue fighting, and has devolved power to the *wiliyets* or local committees, including espousing a 'virtual caliphate' to be conducted online.

(*Continued*)

This is principally taking the form of online propaganda and incitement, the provision of how-to manuals, and fund raising through low-level cyber crime. The threat remains of the *CyberCaliphate* improving their capabilities to provide cyber attack support to amplify the impact of physical terrorist attacks or in the future to achieve their assumed aspirations of spectacular and deadly cyber attacks.

Cyber capability assessments are made by counterterrorism intelligence. These are not made public but are occasionally referenced in official documents or pronouncements. The general consensus of intelligence analysts is that the leading radical Islamic threat groups aspire to carrying out spectacular destructive attacks using cyber techniques, but that the groups' current capabilities fall short of the advanced mastery of cyber-physical controls that would be necessary.[20]

The dispersal of the followers of the Islamic State from the physical territory they had occupied in Syria and Iraq has led to the creation of a 'virtual caliphate' and an increased emphasis on information technology as an enabler to sustain and inspire disparate followers. The dissemination of online propaganda and tactical instruction manuals is a key concern for the authorities, as it incites followers to carry out physical attacks and may improve the effectiveness of terrorist operations. Interventions by the authorities are made to remove hate content and terror-related materials such as recipes for bomb making from websites and social media groups. Terrorist manuals that are available online are commonly doctored by intelligence teams to make them ineffectual or worse. Cyber crime, such as credit card theft, is used by terrorist followers to fund some of their activities, including financing their physical attacks.

Counterterrorism operations are increasingly targeting the cyber capabilities of terrorist groups, deploying offensive cyber attacks that destroy equipment and disrupt networks to systematically degrade their capabilities and to suppress propaganda.[21]

As militant jihadists become more accomplished, it is likely that they will use cyber means to augment and enhance their physical attacks, perhaps providing disinformation or disabling communications to confuse counter-terrorism responders to a terrorist incident. Spectacular and deadly cyber attacks may be an aspiration of these groups, and it is important to monitor any improvements in capability of these threat actors to be prepared for future attacks of this type.

5.2.7 Nation-state- and State-sponsored Cyber Teams

There are many nations around the world that now maintain their own teams of cyber specialists. We identify a cyber team as being nation-state or state-sponsored if it can be identified as part of the state apparatus, funded by the government, or part of a national institution. An important distinction from other types of cyber threat actors is that they are ultimately answerable to their national sponsor, and although they can seem to be acting as though they are uncontrolled and may be operating with deniability, they may be restrained by protocols of international convention and fears of retaliation. A minor distinction is sometimes made between nation-state actors effectively acting as official agents of the state, and state-sponsored teams that may receive national support and endorsement but may be more deniable and only distantly related to official bodies.

State-sponsored cyber teams are typically part of a national security unit or intelligence-gathering organization. They are increasingly linked to military capability and commonly regarded as a fifth branch of the armed services. Various divisions of government have interests in cyber operations, ranging from law enforcement to homeland security, foreign policy and trade, diplomatic corps, and counter-terrorism, so that in more advanced countries cyber units may be attached to some or all of these departments. All of these groups may be conducting different types of cyber operations, ranging from passive data gathering and listening, to offensive attacks to damage the computer networks of people in other countries that they regard as posing a threat.

In Figure 5.1 we list a selection of active state-sponsored cyber teams from 14 countries. These are by no means the only state-sponsored cyber teams operating. Almost all advanced countries with armed forces are maintaining some level of a cyber operations team. We have divided them into countries that either are aligned with Western democratic economies or potentially could be adversarial. Countries listed as adversarial have at some point carried out cyber operations against commercial interests of Western businesses, and have been tracked exploring vulnerabilities in military, government, and critical national infrastructure.

State-sponsored teams are well resourced. Where they have high levels of capability, they are referred to as advanced persistent threats (APTs). Many of the Russian and Chinese teams are labeled as APTs. Different commercial

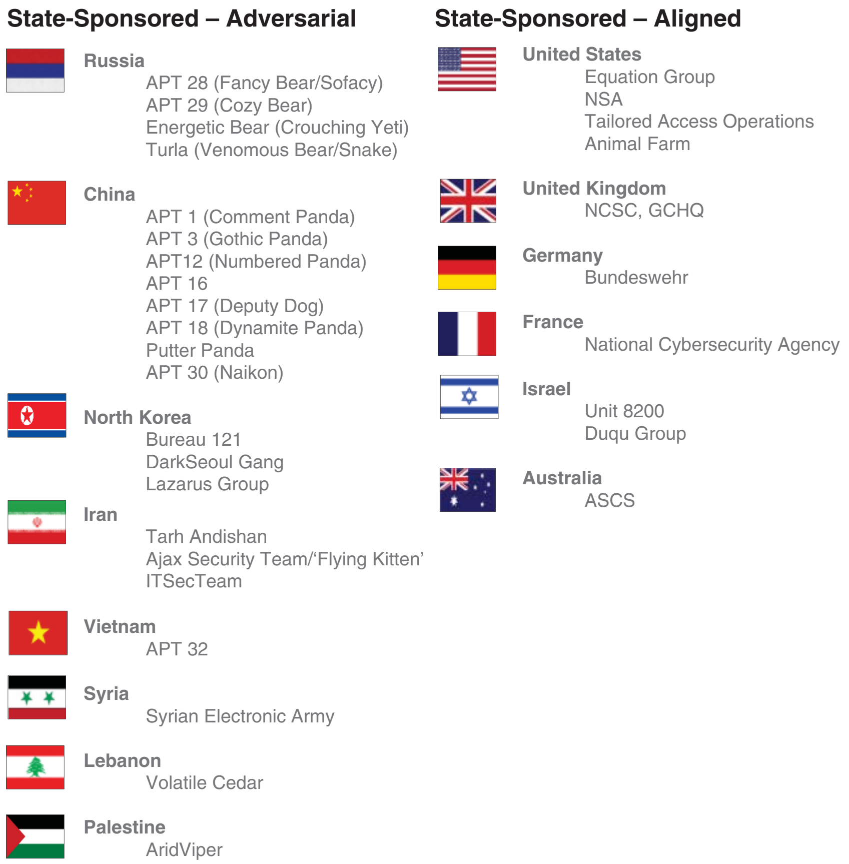

FIGURE 5.1 State-sponsored cyber teams: a selection.

security teams, such as Kaspersky and Symantec, track the activities of these APTs by their use of infrastructure and reuse of software code, and each is given a pet name, so that the same team may be referred to by multiple names.

Nation-state cyber teams are well resourced and have high capability. Most operate as clandestine cyber-spies, but some mount aggressive campaigns of intrusive attacks that infect and damage machines, disrupt business operations, and steal valuable information.

A few state-sponsored teams are responsible for some of the most severe financial thefts, data exfiltration attacks, and contagious malware attacks. It is alleged that *Lazarus Group* was responsible for the highly

STATE-SPONSORED CYBER TEAMS

Energetic Bear **Russian Advanced Persistent Threat (APT) Team**

Energetic Bear has been tracked as a Russian APT team since 2010, so named by Kaspersky Lab because of its clear interest in the energy sector, targeting oil and gas companies.[22] Symantec calls it *Dragonfly*. Kaspersky has proposed that the more recent diversification of the group into broader interests in manufacturing, construction, and IT companies merits renaming it *Crouching Yeti*. You can take your pick.

Energetic Bear focuses on industrial espionage, stealing intellectual property from Western oil and gas businesses, renewable energy, and regulatory information from international energy bodies.[23] It may also have an interest in potential cyber-sabotage of Western energy infrastructure, and in putting tools in place to influence the global energy market.

Energetic Bear is classified as Russian because of build-time stamps in its malware on Moscow standard time, and as state-sponsored because its command-and-control servers operate out of the Federal Security Services (intelligence service) buildings of the Russian Federation.[24] It is assumed to be siphoning Western IP to Russian oil and gas companies.

During the period 2013–2014, *Energetic Bear* ran at least five overlapping campaigns, including spear phishing key individuals, inserting Trojan software into target businesses, running a watering-hole attack to obtain credentials, and creating different types of malware. The group has compromised industrial control system software used in commercial devices, created contagious *Havex* malware that has infected thousands of computers, hacked into more than a hundred organizations, and maintained over 200 command-and-control servers in more than 20 countries. A typical attack infects companies through Windows operating systems, injecting Trojans that connect back to a large network of enslaved websites acting as command and control.

It is estimated that *Energetic Bear* must have at least 350 staff and $1.5 million in capital resources.

damaging 2014 attack on Sony Pictures, attempts to steal nearly a billion dollars from banks via compromising the SWIFT interbanking network in 2016 and 2017, DDoS attacks on South Korean government agencies from

2009 to 2013, the release of the *WannaCry* malware in 2017, and thefts of cryptocurrency. *Lazarus* is so-called because it re-emerges in slightly different manifestations for each campaign but retains characteristic signatures in its malware, of which there are more than 150 known variants.[25] Its operations have involved Chinese middlemen. The attribution of *Lazarus* as a North Korean state-sponsored team is considered highly probable by US government officials, from complex and classified tracing by the US National Security Agency (NSA) of command-and-control signals back to North Korean URLs.[26]

From its operations, *Lazarus* looks more like a cyber criminal organization stealing money and monetizable data assets than following a politically-inspired agenda. The overlap and blurring between what might be a political agenda of destabilizing and punishing organizations that annoy national administrations versus financially motivated campaigns to steal money may be a fine line.

Inflicting cyber loss as punishment or to destabilize opponents or manipulate competitors may be a characteristic of state-sponsored campaigns. The *NotPetya* contagious malware attack in 2017 (described in Chapter 2) was disguised as ransomware but was actually a disk wiper, so was carried out from a motivation of inflicting damage rather than for financial gain, and delivered via a vector in Ukrainian tax reporting software, presumably to target businesses with Ukrainian trading connections. The US, UK, and Australian governments all blamed the Russian military for creating and releasing the malware.[27]

Russian state-sponsored teams *Sofacy* (APT 28) and *Cozy Bear* (APT 29) have been blamed for politically motivated hacks, such as the leaking of the Democratic National Convention's (DNC's) emails in an attempt to influence the 2016 US presidential election.[28] The effectiveness of cyber operations in swaying democratic elections has become a major theme ever since, with a wide variety of allegations of foreign interference, ranging from manipulating social media networks to hacking ballot reporting, in elections all over the democratic world.

Cyber units are used to apply diplomatic pressure and to threaten punitive cyber attacks if intergovernmental relations break down. Following a diplomatic row in 2018 over British allegations that a Russian refugee living in London had been poisoned by Russian agents using nerve gas, fears of a Russian cyber attack as a reprisal prompted an unprecedented public alert from US and UK governments, with instructions on purging suspected Russian malware from IT networks and even domestic routers.[29] There have been fears for some time that Russians have infiltrated dormant and undetected malware into a wide range of IT systems in the West, from commercial business, government, and military systems through to critical national infrastructure, power grids, and utilities, giving the Russians the ability to cripple Western economies at will, in echoes of Cold War paranoia.[30]

Whether foreign state-sponsored cyber agents have already embedded malware in all our systems or not, the Western democracies have become increasingly proactive and aggressive in empowering their state-sponsored cyber teams to go on the offensive and strike back or preemptively. Laws have been passed to enable ‘active cyber defense’ for teams to conduct cyber attacks against foreign targets where it is deemed necessary to do so. Active cyber defense powers have been granted to US NSA groups, to the UK Government Communications Headquarters (GCHQ) National Cyber Security Centre, and amid some controversy for the German military Bundeswehr cyber command. The UK GCHQ cyber attack mandate was first used in April 2018 when it attacked networks and servers of the Islamic State.[31] Other aligned countries are debating the basis in international law and levels of proof required to sanction offensive attack operations by their cyber units. The capabilities and sophistication of the toolkits that have been amassed by Western nation-state cyber teams became apparent in 2016, when an arsenal of exploits apparently used by Equation Group, an NSA cyber team, was published online by a group calling itself *ShadowBrokers*.

It is clear that state-sponsored cyber teams represent a major force in the cyber risk landscape. Some of the more errant and less controlled teams, like *Lazarus* and *Energetic Bear*, are already causing significant losses to Western organizations and our economy. Others could potentially be unleashed by their political masters to cause even more destructive and disruptive impacts under certain circumstances. There are few, if any, organizations that could withstand a concerted cyber attack by a well-resourced and skillful state-sponsored cyber team if the organization is directly targeted.

5.3 THE INSIDER THREAT

5.3.1 Accidents Will Happen

It is natural to focus on the threat from external actors. However, a lot of cyber risk also comes from inside an organization. The internal risk is both accidental and malicious. The large majority of privacy breach events where personal data is leaked and companies have had to pay out compensation have been accidental. Individuals have left their unencrypted laptops in taxis or airports, or have lost memory sticks or other mobile media – even paper printouts – with key data sets on them. Even if a criminal doesn't find the lost data set, the incident still has to be reported to the regulator and all the procedures followed and compensations paid. In the decade before 2013, over half of all privacy breach data loss events were from accidental losses. The advent of password-protected laptops and standard practices of encrypting data sets in transit have rapidly cut the incidence of accidental data loss. Now less than 20% of data loss incidents come from accidental causes – two-thirds are from malicious external actors.

5.3.2 Human Vulnerability of Your Staff

The personnel of an organization are the unwitting vectors of many of the cyber incidents that occur. An employee clicking on a bogus link in a phishing email or browsing on the wrong website can trigger a new malware infection. The larger an organization with more employees, the more chances there are for one of them to be fooled and enable a cyber loss to occur. When analyzing cyber risk, the strongest characteristic of a company that correlates with likelihood of having a loss is the number of employees it has, for this very reason.

The human vulnerability of an organization is just as important as the technology deployed for IT security. Personnel are recognized as being the human firewall that protects the company.[32] Improving cyber risk awareness of the staff is a growing focus of security measures, and there are various ways of scoring the awareness level of employees, monitoring metrics of improvements over time, and benchmarking against industry sector averages and an organization's peers, that are worth instituting in any business with significant cyber risk.

5.3.3 Disaffected Employees

A small proportion of cyber loss incidents to a company results from the deliberate act of an employee. Since records of cause began in 2005, around 10% of regulatory-reported data loss events each year have been attributed to the malicious acts of insiders.

Insiders may be acting for financial gain, or may be acting through motives of whistle-blowing to publicize activities of the organization they disagree with, or acting to punish their employer. There are many examples of employees acting against the best interests of their employers, including theft, fraud, vandalism, and sabotage. This is known as 'workplace deviance', and is heavily under-reported. Insider cyber crime is a growing area of study to understand the root causes, the circumstances, and the characteristics of employees who carry it out. Surveys of workplace deviance acts of cyber crime suggest that most insiders were acting out of revenge, often triggered by perceived insults by or being treated unfairly by their employer, with motivation related to a negative work-related trigger event.[33]

INSIDER THREAT

The Disaffected IT Engineer

Statistics of unauthorized cyber activities by employees causing harm to organizations suggest that most are caused by motives of revenge arising from perception of being treated unfairly, and are usually triggered by a negative work-related event, such as being reprimanded, demoted, or laid off. Organizational factors may enhance employees being aggrieved, such as job stress, organizational frustration, lack of control over work environment, and weak sanctions for rule violations. Most of them have complained to colleagues openly in the workplace about their grievance prior to their action. Two-thirds of them act after they have resigned, or simultaneously with their termination. Roughly equal numbers resign or are fired.[34]

Eighty-six percent of them are in the IT department or are in technical roles in the organization, and 10% are professional positions elsewhere in the organization. Common actions include compromising computer accounts, creating unauthorized backdoor access paths or fake accounts, taking copies of sensitive data or protected personal information, or using shared accounts in their attacks.

5.4 THREAT ACTORS AND CYBER RISK

5.4.1 Threat Actors and Their Variety Act

We have described some of the main categories of cyber threat actors. There are, no doubt, other types of individuals who can pose a threat. (There may, for example, even be skilled IT teams or individuals in a company's competitors that may not be above carrying out a sneak attack if it gets them a minor advantage, and they think they won't get caught.) Threat actors have a wide range of skill levels and motivations.

These ecosystems of different cyber threat actors interact, feed off each other, and together may represent a population of several millions of individuals around the world who are engaged in criminal activity to cause cyber losses to businesses and society.

If you are concerned about protecting your organization from a cyber attack, then your red teaming exercise needs to consider each of these threat actors. Where would your organization rank in the targeting prioritization of each of these groups? Do you represent a target that holds reams of personal data that would be a prize for the organized crime groups that specialize in data theft? Do you deal in volumes of credit card transactions that would be a key attraction for hub-structured cyber criminal gangs? Do you carry out financial transactions that could be a motivation for hierarchically-organized cyber criminal syndicates to infiltrate? Does your organization carry out practices that could make it a target for a hacktivist? Could your business be the focus of a state-sponsored attacker interested in espionage of industrial secrets or punishing your organization for its business dealings?

5.4.2 Cyber Criminology

Criminology is the science of criminal motivation, causes, and control.[35] To solve cyber risk in society, we need to understand the motivations and deterrence of the people carrying out cyber attacks. Cyber crime challenges many of the conventions of other types of crime: cyber criminals are highly educated, middle-class, and do not fit many of the characteristics of deprivation-induced crime and marginal populations, so theoretical bases for cyber criminology are still evolving.[36] Many of the theorists agree on variations of rational choice theory for the underlying understanding of choices and motivations. This suggests that threat actors are driven by rational choice and weigh costs and benefits when deciding whether to commit cyber crime – essentially, they think in economic terms. Cost is expressed in terms of risk to the actor: the likelihood of being caught and punished is the key deterrence.

The burgeoning industry of cyber crime demonstrates that the risks are currently low relative to the benefits that can be gained. Cyber crime is still met with little deterrence – with extremely low conviction rates for perpetrators. Cyber crime statistics show that in the United States less than 1 in 200 reported cases of cyber identity theft resulted in a criminal case being brought, and only 1 in 50,000 resulted in a conviction.[37] In contrast, armed robbery in the United States results in conviction rates as high as 1 in 5.[38] Even if convicted, cyber criminals face short sentences as judges are still struggling to determine whether harm was caused by stealing data, and what a reasonable punishment should be.[39]

Solving cyber risk will entail increasing the likelihood of being caught, making punishments appropriate to the harm, and establishing deterrence that will rebalance the rational choice for threat actors more towards legitimate use of their talents and away from perpetrating crime.

5.5 HACKONOMICS

5.5.1 Cyber Black Economy

So if the risks of apprehension, conviction, and sentencing for a cyber criminal are so low, how about the rewards? How much do threat actors make from their endeavors, and what levels of effort and skills are required to generate what levels of rewards?

The cyber black economy consists of operations on the internet that generate illegal money flows for commodities and services. This economy is an ecosystem where illegal activity thrives and enables interaction between suppliers and customers for these goods.

5.5.2 Dark Web Trading Sites

Online black markets allow cyber criminals to buy cyber attack tools such as malware and botnets, along with illegal firearms and drugs, and stolen credit card and other information, using cryptocurrencies like Bitcoin, Ethereum, Litecoin, and Monero for transactions.[40] Dark web black markets function like other legitimate online markets, with auction sites, e-commerce, and swap activities.

Large exchanges are periodically discovered and taken down by law enforcement, which reduces trading activity until another site takes over. In 2017, *AlphaBay* (once known as the Amazon of the dark web) and *Hansa Market* were closed down by the US Department of Justice in a major international operation. *AlphaBay* was reported to have daily postings of 300,000 listings of stolen credit cards and digital data thefts, along with drugs and other contraband items, generating up to $800,000 a day in revenue.[41] Although other black markets sprang up to take their place (look-alike trading site *Empire Market* was launched only months later),[42] the disruption of revenue streams to cyber criminals has proven highly effective in reducing their capabilities. The closure of the original flagship dark web trading site *Silk Road* in 2013 generated many more sites for drug trafficking and cyber tool sales, including *Black Market Reloaded*, *Sheep Marketplace*, *Atlantis*, *Agora*, and *Silk Road 2.0*, many of which were closed down in turn, or occasionally ceased operations because – guess what – they got conned by the con men running them.

5.5.3 Dark Web Prices

Typical prices of products being offered for sale on trading sites on the dark web are shown in Table 5.1. These prices vary according to supply and demand. Analysts watching the prices on these sites can sometimes tell when a large cache of stolen data has hit the market because the prices fall. Avoiding flooding the market with large data sets may be one constraint for cyber criminals in planning large-scale data exfiltration attacks.

An analysis of provision of online 'booter services' websites that offer denial of service attacks for a fee concludes that payment by PayPal is generally possible; however, alternative payment options are usually available, including digital currencies such as Bitcoin. Entry-level pricing allowing 10-minute attacks on one target at a time was typically priced at less than US$5 a month.[43]

5.5.4 Logistical Burden of Cyber Attacks

Putting a successful cyber attack together requires resources. It takes skills, time, people, equipment, and some amount of money. Of these, the level of skill and expertise is probably the most critical. Table 5.2 suggests a scaling for the skill levels of operatives that may be involved in a typical attack.

Cyber attacks can be assessed by the level of difficulty, or 'logistical burden', needed to carry them out. This estimates the numbers of people with different levels of skills needed to work together to write the malware code, do reconnaissance on the targets, explore entry points and vulnerabilities, do the social engineering to find someone who will inadvertently provide a way in, implement the attack itself with sufficient proficiency to minimize detection, and fence or money launder the proceeds.

The logistical burden assesses an index for the attack, using notional costings for personnel with different skills needed, for certain durations, and for the costs of utilizing equipment and obtaining technology tools. Estimates of the total logistical burden make it possible to estimate the total effort required for teams to mount campaigns of cyber attacks, monetized into dollars. Many of the attacks that we have analyzed required a logistical burden index value of between $100,000 and $2 million. Some of the more sophisticated financial transfer attacks have index values

TABLE 5.1 Prices of commodities available on dark web black market sites.

Item	Details	Price on dark web
Fullz	Complete sets of personally identifiable information (PII) for an individual, usually including Social Security number	$1–$8 (US citizen); bulk discount available Fullz with credit card, PIN number, and bank account details: $30 (US)
Credit card details	Card transaction credentials taken from malware, point-of-sale terminals, or online transactions. Typically includes card number, expiration date, cardholder name.	Individual cards: $2–$20 Dump prices: $5–$100
Bank account details	Online bank account details, including balance and access credentials	Priced according to balance in account, e.g. $100 for details of account with balance of $1,000; $1,000 for details of account with balance of $20,000
Subscriptions	Netflix subscription or PayPal credentials	$0.50
Exploit kits	User-friendly pre-written software, including ransomware, Trojans, and malware	Licensed for $80–$100 a day, $500–$700 a week, and $1400–$2000 a month
DoS-for-hire	Denial of service attack botnet networks	From as low as $1 an hour Booter services (DoS on behalf of customer): $5–$30 an hour Attacks on military, government, or bank websites: $100–$150 an hour
Remote desktop protocols (RDPs)	Compromised RDP providing a vector for initial entry penetration of a network	Around $10, but varies by type of network

Source: Rowley (2017); Dark Web News (2017).

TABLE 5.2 Skill level gradings for cyber hackers.

Level	Type of Hacker	Experience
1	Amateur or entry-level hacker (ELH)	High school or in higher education
2	Coder or software engineer (CS)	Science degree, or at least years of amateur coding
3	Experienced coder (EC)	More than five years of professional experience, possibly with zero day development experience
4	Highly experienced coder (HEC)	More than 10 years of professional experience, possibly with experience in industrial control systems
5	Integration engineer and systems architect (SA)	Project design skills and ability to manage software development teams of up to 10
6	Senior technical operations lead (STOL)	Large project conceptualization and management, with ability to manage software projects of very large teams

above $5 million. These logistical burden index values can be thought of as a notional budgeting cost without sunk costs or standing commitments, and at professional charge-out rates – i.e. what it would cost to hire a team to carry out this type of attack. This is done simply to benchmark and compare the effort and skill requirement of one type of cyber attack with another.

This type of analysis identifies the ‘hackonomics’ of carrying out attacks as a rational actor seeking reward for the investment of resources. Some types of threat actors do not have the ‘logistical budget’ – skills, capabilities, and resources – to carry out attacks above a certain index value. Some attacks do not provide a good enough return to merit a threat actor investing effort in them.

Overall, we can see that a few hackers must be making a lot of money from cyber crime, but the large majority of hackers seem highly unlikely to be generating earnings from their skills that would be comparable with what they could earn with the legitimate use of their skills in employment. Some of this may be lifestyle and cultural choices, but if we could find ways of helping hackers find legitimate channels for reward from their talents, everyone might win.

5.5.5 Hackers Are Rational Game Players

Overall, in designing security systems and considering how best to manage the threat of cyber attacks, it is useful to consider the risks and rewards of the attacks from the hackers' point of view. They may well want to attack you, but they will take a more attractive or easier target if there is such an alternative available. They have finite resources, and they are looking to get a return on the effort they will invest.

By the principles of deterrence, you don't need to make their task impossible. Just to make it not worth their effort. Make the risk-return ratio unworthwhile for them. Most of what we know about hackers leads us to believe that they are rational game players.

To solve cyber risk, we need to play them at their own game.

ENDNOTES

1. CCRS (2018d, Smith et al).
2. Poulsen (2009).
3. Squatriglia (2008).
4. Carr (2008).
5. CCRS (2018d, Smith et al.).
6. BankInfoSecurity (2006).
7. BankInfoSecurity (2006).
8. Broadhurst et al. (2014) and Kshetri (2010).
9. McGuire (2012).
10. Broadhurst et al. (2014) and Kshetri (2010).
11. Bhattacharjee (2011).
12. Bing (2017); ABC News (2017).
13. RSA (2017).
14. Meyer (2018).
15. Doherty et al. (2013).
16. Danchev (2012).
17. InfoSEC Institute (2016).
18. See chapter 'The New Media' in Hoffmann (2006) and see Weimann (2006).
19. The US National Academy of Sciences first warned of a 'digital Pearl Harbor' as early as 1990; see Weimann (2004).
20. CCRS (2017b).
21. BBC (2018).
22. Kaspersky Lab (2014).
23. Symantec (2014a).
24. Symantec (2014b).

25. Kaspersky Lab (2017).
26. Schwartz (2017).
27. Heller (2018).
28. Khandelwal (2017).
29. Kirkpatrick (2018).
30. Perlroth (2018).
31. BBC (2018).
32. Cyber Risk Aware (2017).
33. *E-Crime Watch Survey* reported in Keeney et al. (2005).
34. CCRS (2018e, Daffron et al.).
35. Treadwell (2013).
36. Jaishankar (2011); and see also the *International Journal of Cyber Criminology*.
37. FBI IC3 (2016).
38. Grimes (2012).
39. Williams (2016).
40. PYMNTS (2017).
41. Greenberg (2017).
42. *Dark Web News* (2018).
43. Hutchings and Clayton (2016).