القمة العالمية للحكومات
WORLD GOVERNMENT SUMMIT

In Collaboration With

pwc

A PRACTICAL METHOD OF IDENTIFYING CYBERATTACKS

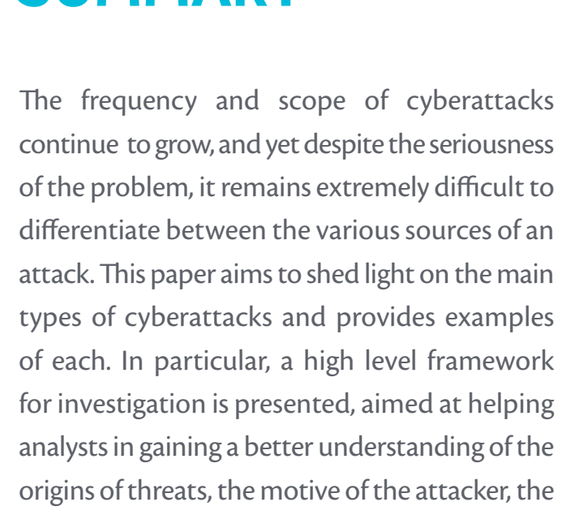
February 2018

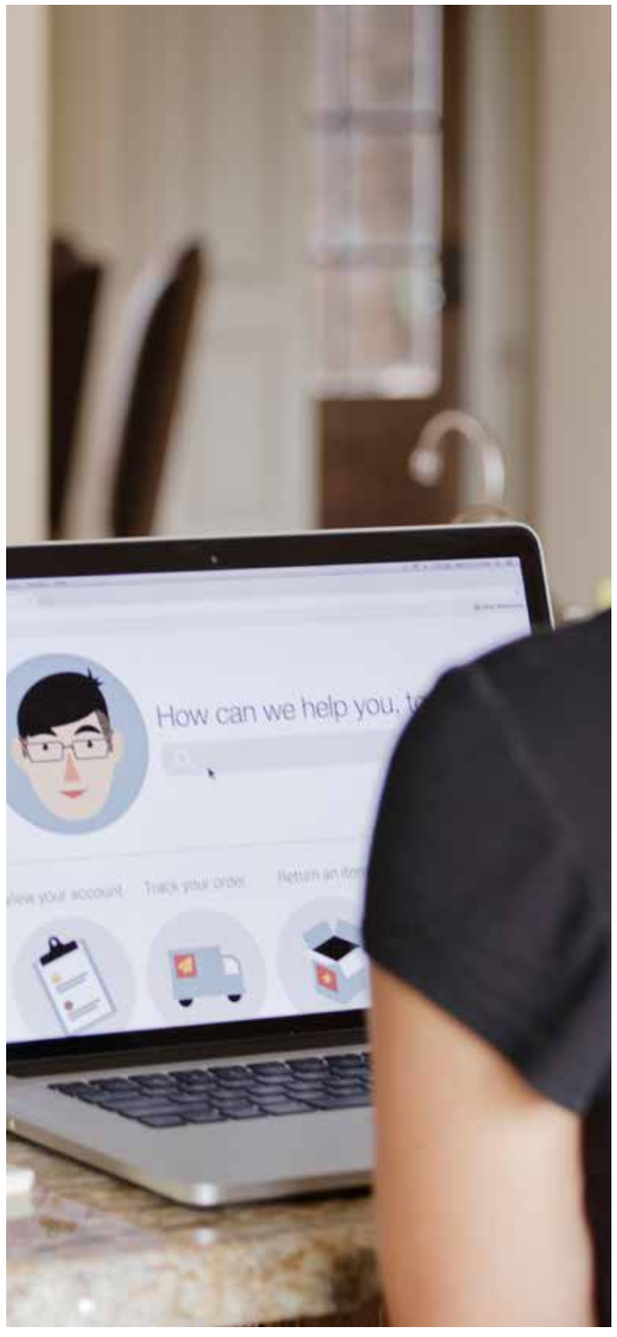
INDEX

TOPICS

EXECUTIVE SUMMARY

The frequency and scope of cyberattacks continue to grow, and yet despite the seriousness of the problem, it remains extremely difficult to differentiate between the various sources of an attack. This paper aims to shed light on the main types of cyberattacks and provides examples of each. In particular, a high level framework for investigation is presented, aimed at helping analysts in gaining a better understanding of the origins of threats, the motive of the attacker, the technical origin of the attack, the information contained in the coding of the malware and the attacker's modus operandi. Nonetheless, attribution will continue to be difficult, which makes the study of the topic more urgent than ever before.





OVERVIEW

Cyberattacks carried out by a range of entities are a growing threat to the security of governments and their citizens. There are three main sources of attacks; activists, criminals and governments, and - based on the evidence - it is sometimes hard to differentiate them. Indeed, they may sometimes work together when their interests are aligned. The increasing frequency and severity of the attacks makes it more important than ever to understand the source. Knowing who planned an attack might make it easier to capture the culprits or frame an appropriate response.

Figure 1: Overview of common threat actors

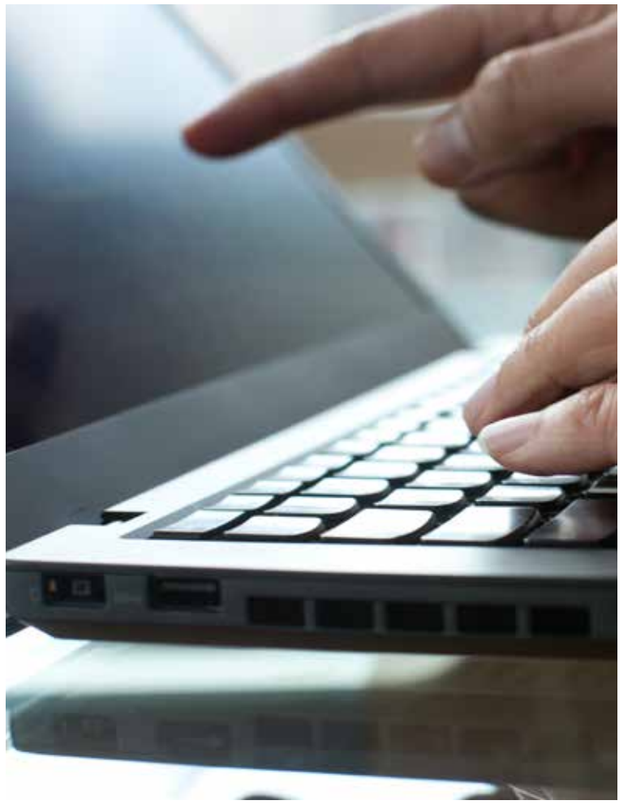
Actors	Motives	Impact	Further characteristics
Governments	Economic, political, and/or military advantage	Loss of competitive advantage Disruption to critical infrastructure	Major budget Extremely sophisticated Willing to hide real motive and eventually direct public opinion or retaliation towards a specific outcome
Criminals	Immediate financial gain Collect information for future financial gains	Costly regulatory inquiries and penalties Consumer and shareholder lawsuits Loss of consumer confidence Financial loss	May or may not be organised Interested in covering their traces in order not to be prosecuted Different criminal actors may constitute the whole attack "supply chain"
Hacktivists	Influence political and/or social change Pressure business to change their practices	Influence political and/or social change Pressure business to change their practices	Usually less organised than other actors Tend to perform simpler attacks with lower budget (such as Disturbed Denial of Service or DDoS) Usually interested in being recognized as the source of the attack

In addition, there is a risk that a cyberattack may be misattributed or mistaken for a government-sponsored attack and spark a broader cyber or physical war. Alternatively, a government-sponsored hack may be disguised as a case of cyberactivism or cybercrime to avoid a government-to-government response.

The classification of a cybersecurity event into different categories is mostly dependent on the motive for the attack. In cases in which the attack is motivated by political factors, the cyberattackers often have a strong interest in hiding the real reason behind it. Alternatively, when the motive behind the attack is financial, the actors behind it are less interested in disguising the motive than in making it difficult for law enforcement authorities to find the perpetrators. Given this complexity, different approaches need to be applied to identify the actors behind a cybersecurity event.

This paper will provide examples of the different types of cyberattacks and an analytical framework intended to help governments differentiate the source of such threats, even though the tools of the attackers, the people involved in the attacks and their target may be the same.

With this in mind, this paper describes some important cybersecurity-related events and their attribution. It goes on to offer different approaches that can be used to attribute a large-scale and complex cybersecurity related event. Finally, it provides a framework for the analysis of events related to cybersecurity to help discern the difference among the types of cyberattack.



THE RESPONSES TO A GROWING THREAT

As governments and industries around the world become digitally enabled, the number of cybersecurity-related events has grown rapidly. It is worth providing some statistics on the scale of the problem, for organisations and individuals to defend themselves from an attack, and for the authorities to catch the perpetrators.

In 2016, Cybersecurity Ventures, a US research firm, predicted that cybercrime will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015. The average cost to an organisation of a data breach was $3.6 million, based on a 2016 survey of 419 companies in 13 countries conducted by the Ponemon Institute, a US research firm.

The global cost of the damage caused by one form of cyberattack, ransomware, is predicted to exceed $5 billion alone in 2017, a 15-fold increase in two years, and is expected to worsen. Ransomware attacks on healthcare organisations-an industry which has been targeted by major ransomware campaigns in 2017-will quadruple by 2020. Cybersecurity Ventures predicts that a business will fall victim to a ransomware attack every 14 seconds by 2019.

Also, according to the Computer Crime and Intellectual Property section of the US Department of Justice, ransomware is the fastest growing malware threat[1], targeting users of all types, from the home user to the corporate network. On average, more than 4,000 ransomware attacks have occurred daily in 2016. This is a 300-percent increase over the approximately 1,000 attacks per day seen in 2015. According to a PwC Global analysis of economic crime, cybercrime is now the second most reported economic crime, affecting more than 32% of organisations worldwide[2].

[1]https://www.justice.gov/criminal-ccips/file/872771/download
[2]https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html

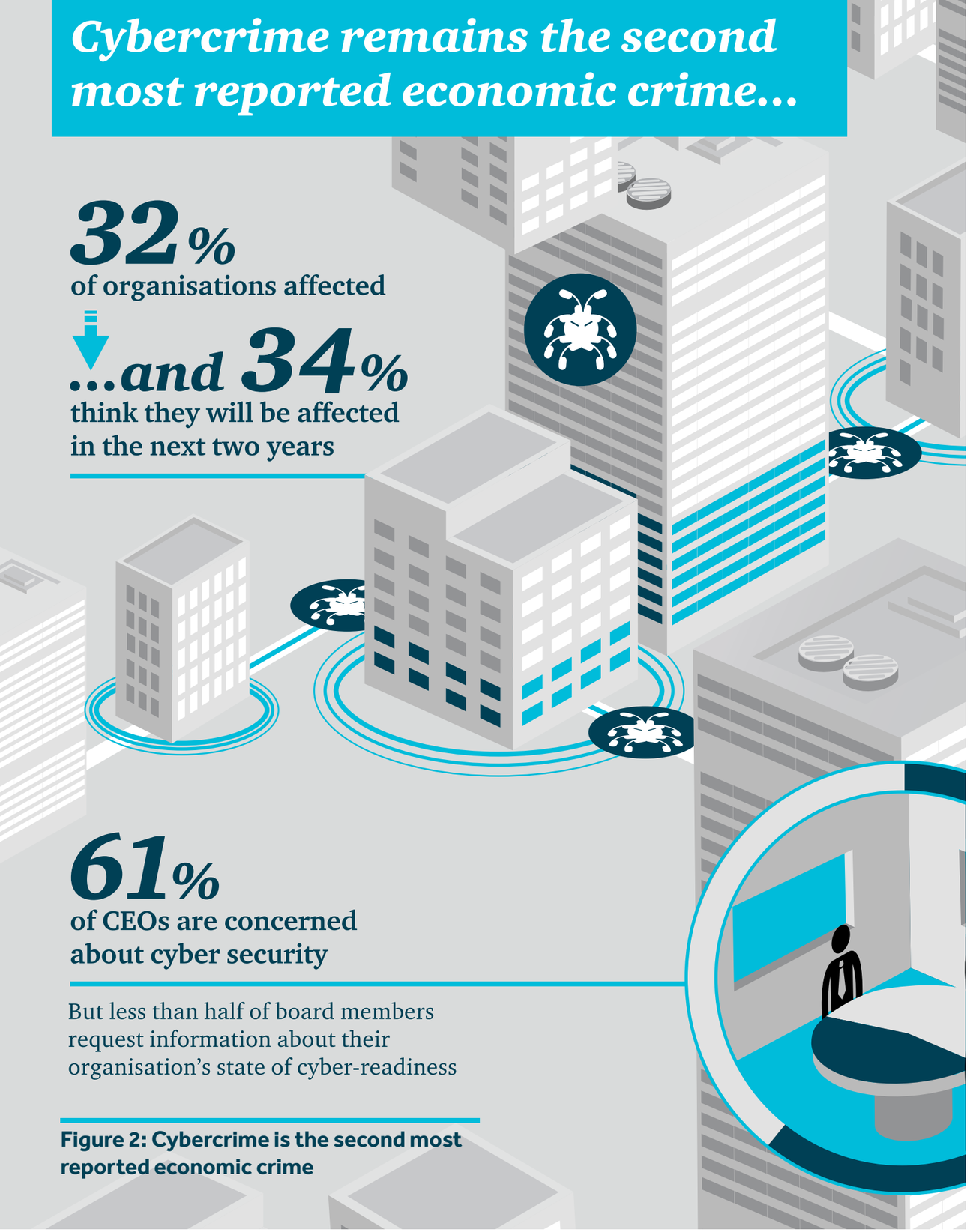


Figure 2: Cybercrime is the second most reported economic crime

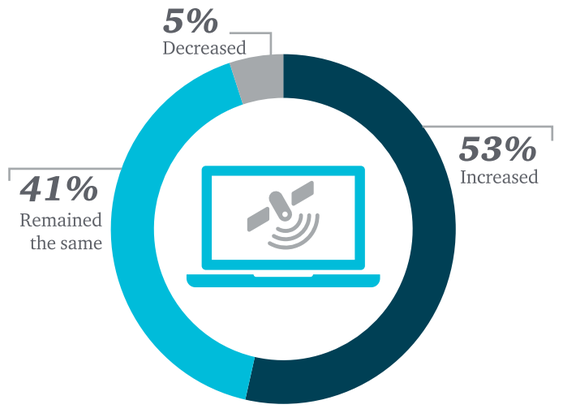
PwC 19th Annual CEO Survey

Furthermore, in the same report, PwC highlights an increase in public awareness of cybercrime. This is mainly due to widely publicised and successful cyberattacks, and to the fact that many countries have enacted regulations forcing companies to report cyberattacks, even if the consequences of the attacks are not always made public.

As a result of these changes in the threat environment, global spending by organisations and individuals on cybersecurity measures is expected to exceed $1 trillion over a period of five years to 2021, according to Gartner, a US research firm. The rising tide of cybercrime will push spending on information security to more than $86 billion in 2017, the firm predicts. This amount does not include some individual cybersecurity subcategories such as Internet of Things (IoT), Industrial IoT, Industrial Control Systems (ICS) security and automotive security.

As the world relies more on digital technology, the size of the target for cyberattackers grows. There are 3.8 billion internet users in 2017, just over half the world's population, compared with 2 billion in 2015. Cybersecurity Ventures predicts there will be 6 billion internet users by 2022 and more than 7.5 billion internet users by 2030. Efforts to mitigate the risk of cyberattack are struggling to keep up with the threat.

Figure 3: Perception of the risk of cybercrime (in comparison to 2014)



Demand for people with cybersecurity skills outstrips supply. Combatting cyberattacks will lead to more than triple the number of unfilled cybersecurity jobs worldwide, which is predicted to reach 3.5 million by 2021, according to CyberSecurity Ventures. In the US alone, there were 350,000 cybersecurity job openings in late 2017, compared with nearly 780,000 people employed in cybersecurity positions, according to CyberSeek, a project supported by the National Initiative for Cybersecurity Education, a program of the National Institute of Standards and Technology in the US Department of Commerce.

DIFFERENT TYPES OF PERPETRATORS

Most of the statistics that are publicly available focus on the targets of attacks and the way they are carried out; very little analysis is conducted on the perpetrators and their motivations. This is because it is easier to observe the consequences of cyberattacks than to attribute the sources of such events and the motives for carrying them out.

Cyberattacks on organisations (governmental or private) and on individuals fall under three main categories:

1. **Crime:** to steal money from consumers, companies or institutions, in a direct or indirect way, using digital methods. This can include stealing payment information in order to buy or sell goods, seizing the computational power of a target in order to use it for one's own advantage, and so on.

2. **Warfare:** to attack or otherwise destabilise a nation state or its institutions. In many cases, these events are acts of war, but they may also include actions which are more indirectly aimed at spreading alarm or discontent in the population or radicalising positions in the domestic political debate. Also, in this category are cyberattacks carried out by terrorists to cause panic and disruption in a nation state in an attempt to promote a specific political agenda.

3. **Activism:** to protest against real or perceived actions undertaken by governments, corporations or other entities.

Figure 4: Cybersecurity related events, classified by goals

Examples of these three categories are discussed in the following sections of this paper.

THE SCOURGE OF CYBERCRIME

Cybercrimes take a number of different forms. They include the theft of payment-related information (including credit card numbers and other credit card data), such as a cyberattack on more than 1,000 properties belonging to the InterContinental Hotels Group that the company disclosed in April 2017. In that case, equipment at points of sale was compromised with malicious software designed to siphon out customer debit and credit card data.

In mid-2017, the US consumer credit reporting agency, Equifax, suffered a cyberattack that resulted in the leakage of personal information, including social security numbers, belonging to more than 145 million users. The information could be used to open a fake bank account in a person's name or to request a loan or mortgage by impersonating a legitimate account holder.

Other types of cybercrime include the hacking of personal, corporate or even national banking accounts to execute money transfers. One example is the attack perpetrated against Bangladesh Bank, the central bank of Bangladesh, in February 2016, when instructions from criminals to transfer $951 million were issued via the SWIFT network. Another case is the attack perpetrated in July 2017 against UniCredit, Italy's largest bank, in which biographical and loan data were stolen from 400,000 client accounts.

THE EVOLUTION OF CYBERWARFARE

Definitions of cyberwarfare vary greatly, reflecting its novelty. Some countries adopt a narrow definition of what cyberwarfare consists of and focus on hacking and damaging systems. Others regard it as part of a wider information warfare that includes not only hacking but also disinformation and propaganda.

Some recent examples of cybersecurity events that fall into the category of cyberwarfare, and are probably to be attributed to a nation state, include attacks in 2013 against three South Korean television stations and a bank, allegedly carried out by hackers belonging to the North Korean government. Another example is the so-called BlackEnergy malware attack, purportedly carried out by hackers widely believed to be tied to the Russian government, which temporarily shut down part of the Ukrainian power grid in December 2016. The event left more than 200,000 people temporarily without power and shut down the business of a mining company and large railway operator.

In August 2013, a number of US companies, including the New York Times, Twitter and the Huffington Post, suffered a cybersecurity breach that caused them to lose control of some of their websites for a time. The source was reportedly found to be hackers supporting the Syrian government who had breached the Australian internet company that manages many major website addresses. A Syrian based hacking group, claimed credit for the Twitter and Huffington Post hacks. Electronic records showed that NYTimes.com, the only site with an hours-long outage, redirected visitors for a time to a Syrian-controlled server.

In other cases, hacking groups, claiming to represent Pakistani nationalist interests, allegedly defaced many websites including Indian, Chinese and Israeli companies, as well as government organisations.

CYBERACTIVISM: ACTIVE AS EVER

Cyberactivism includes cybersecurity-related events aimed at protesting real or alleged actions by governments, corporations or other organisations. Most of the attacks performed by this category of actors are perpetrated using what is normally defined as a Distributed Denial of Service (DDoS) Attack. This kind of attack involves the use of a set of computers or devices which have been previously hijacked to direct traffic toward a single target website, with the aim of saturating the network or computational capacity of the target and, thus, render the website unreachable. In less frequent cases, hacktivism is perpetrated by defacing websites or publishing private information on the Web. Defacement attacks are executed by hacking the hosting infrastructure of public websites and putting different content in lieu of the usual victim's website, while the private information to be published can be acquired in a range of different ways, including the use of insiders to acquire data without performing specific cyberattacks.

Recent examples include hackers supporting the Catalan independence movement targeting websites run by Spain's Ministry of Public Works and Transport in 2017. Some sites were defaced to display a "Free Catalonia" slogan, and others were bombarded with DDoS attacks. In the previous year, a hacktivist group launched DDoS attacks on several Thai government websites to protest against proposed laws that would allow the government to censor websites and intercept private communications without a court order.

Among the best known hacktivist groups is Anonymous, a loosely associated international network of hackers that has launched DDoS attacks since 2003 against government, religious and corporate websites. The group has portrayed itself as an advocate of broader humanitarian causes, but many recent attacks have earned it negative publicity, because of its association with various non-state attacks against governments around the world.

Hacktivist entities such as Anonymous are not fully fledged organisations, but rely on different cells with different skills and final objectives. Thus, state actors or criminals have often hidden their origins by pretending to be part of these loosely organised networks. Even in the cases in which specific hacking groups linked to Anonymous have been involved, the attacks were claimed by different parts of the organisation and the effects of the attacks were highly exaggerated.

THE ATTRIBUTION PROBLEM

Many of the difficulties that arise in classifying a cybersecurity-related event are linked to the fact that attackers do their best to hide their true identity. The perpetrator wants to protect himself or herself from prosecution and the attack may be politically motivated, in which case attribution may lead to retaliation against the perpetrator, such as a national government. By the same token, a fundamental concept in cybersecurity and digital forensics is the fact that it is sometimes extremely difficult to identify the perpetrator after a cyberattack has been committed. Hackers have a lot of technical tools at their disposal to cover their tracks. And even if analysts are able to identify the origin of an attack, this does not automatically mean they are able to point to the perpetrator.

This is known as the attribution problem. The difficulty in identifying the root cause of an attack, and attributing it to a particular hacker or group of hackers, has gained attention in recent years as the number of cyberattacks has been increasing. This can amplify the consequences of some cyberattacks by potentially prompting a government to retaliate against the wrong actors and, possibly, lead the public to the wrong conclusion. In democratic countries, such as the US, if the intelligence community agrees on an attribution, and is ready for the administration to share it publicly, citizens request proof or an explanation of how the attribution was reached.

That said, it is worth noting that the release of information about technical and physical intelligence capabilities and initiatives can undermine current and future operations. As a result, even in cases in which intelligence agencies are able to make a determination with a strong degree of confidence, they encounter additional difficulties when the findings are made public.

Clearly, there are cases in which it is impossible to come to a clear conclusion in digital forensics, given the amount of available information. Yet, experience suggests that in most cases, a relatively certain attribution can be found based on the available information. Sometimes, it is possible to publish the full background information which may, however, create further problems in sharing such findings.

A case in point occurred when the US administration accused North Korea for the cyberattack on Sony Pictures in 2014. Much of the security community agreed with the consensus that North Korea was the source of the attack, but there were also some prominent skeptics. This was due, in part, to the fact that President Obama did not disclose whether the US had the ability to spy on North Korean internet activity before and during the attack on Sony's computers. The ability to spy on North Korean internet activity was partially disclosed later by the New York Times, but without confirmation by the US government. In this case, as in many others, partial access to evidence makes it difficult for individuals and civilian security firms to assess government attributions.

On the opposite side of the debate, president-elect Trump in December 2016 highlighted the same attribution problem to hamper the formation of a consensus about political hacking during the presidential campaign. Speaking to FOX News, he said, "Once they hack, if you don't catch them in the act you're not going to catch them. [American intelligence agencies] have no idea if it's Russia or China or somebody. It could be somebody sitting in a bed some place. I don't really think it is [the Russian government], but who knows? I don't know either. They don't know and I don't know."

In a broader sense, the attribution problem applies to any type of investigation, not just a digital forensics one. A direct proof of who committed a crime is not always available and it can be difficult or even impossible to discern a perpetrator from the evidence and information available. Nonetheless, it is possible to codify a justice system that identifies suspects and then decides whether they are innocent or guilty of crimes based on available evidence. In the absence of perfect information, a justice system will certainly make inaccurate determinations from time to time, but if the overall rate of success is generally perceived to be satisfactory, the system is sustainable.

Although cyberattacks and digital attribution are in their infancy compared with physical crimes, systems for cyber attribution are slowly developing in the same way. Since attribution is based on degrees of certainty, not absolute levels, people's confidence in the reporting of the perpetrators and their motives continues to evolve. "Attribution is extremely difficult and requires intelligence sources that are reliable and accurate," says David Kennedy, CEO of the security firm TrustedSec, who formerly worked at the National Security Agency and with the Marine Corps' Signal Intelligence unit. "The intelligence community typically monitors specific groups and activity in order to have high confidence. It's not a perfect system"[3].

[3]http://www.marketingcyber.com/attribution-does-it-really-matter/

TRACKING THE ORIGINS OF CYBERATTACKS

In order to track the origin of a cybersecurity related event, and then to categorise correctly, the attacks need to be analysed from a number of viewpoints. These include:

1. Motivation: The typical question is whether a possible incentive exists for the actor to perform the attack. Once a potential incentive has been identified, it is important to discern whether the activity can match the specific incentive, in order to validate the hypothesis.

2. Technical origin of the attack: This includes such information as the location of the devices used for the attack, any command-and-control IP address, the email address or other channels required for paying a ransom.

3. Information included in data files, binary codes and scripts: This is only applicable in cases in which a specific malware or customised exploit is used. In these cases, this information can include the used compiler, libraries and other technical information for the binary code. The scripts usually provide more information, as they may include comments and other information in the natural language used by an attacker (including dialects and slang, which pinpoint the attacker). Based on the script programming style, it may be possible to understand if the script has been produced by a known coder. Also, the file names may provide tell-tale information, as they usually include natural language, often dependent on the writing style of the coder.

4. Analysing the modus operandi of the attacker: This includes:

- Matching the hours when a hacker is active with a particular location. This may indicate the location from which the attacker is operating.
- Script comments, if available, may provide information about the language or even slang used by the attacker.
- Malware tactics, if similar to the ones used by a known actor, may indicate that this particular actor was involved.

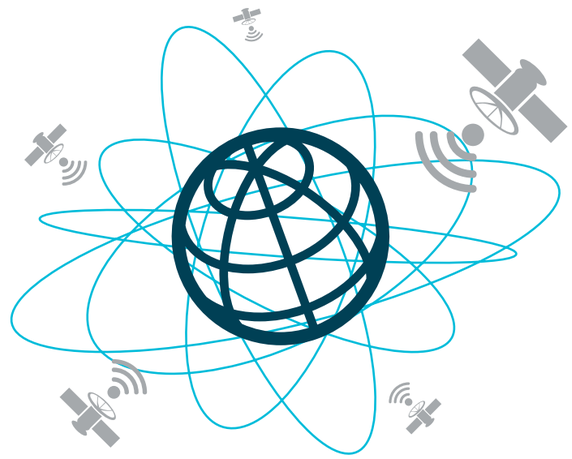
Motivation	Identify if the alleged actor has a rational incentive for performing the attack
Technical origin of the attack	Tracing down information such as the location of the devices used for the attack; any command-and-control IP address, the email address or other channels required for paying a ransom
Information included in the binary code and scripts	Analyse technical data such as the used compiler and libraries for the binary code, and natural language information in the comments of the scripts, plus the style of programming, which can be used to identify if the code has been written by a known coder File names can also reveal the language or slang the attacker is using
Modus operandi	Analyse the hours when a hacker is active, as they may indicate the location from which he is operating Malware tactics, if similar to the ones used by a known actor, can indicate that the actor was involved

Nonetheless, the usage of the same methods and tactics as those of a known actor is a reasonable indication of the identity of an attacker. For example, some of the hacking groups prefer to gain domain administration rights on Windows servers and create multiple backdoors. In contrast, others prefer to compromise only the accounts they need for a particular goal and never write malware to disk, in order to minimise the chance of discovery by endpoint protection software. Also, vulnerabilities usually follow patterns: One hacking group may focus on exploiting font file vulnerabilities, while another prefers to exploit holes in different technologies, such as Adobe Flash. Individuals in hacker groups develop specialties and these specialties can determine the organisation's operational preferences.

It is sometimes possible to identify the group accurately by analysing the combination of tactics, malware reuse and goals. One example of this is Stuxnet, a malicious computer program that caused substantial damage to Iran's nuclear program and was reported in the media in 2010. It is thought to be the work of the governments of the US and Israel. Only a very limited number of groups have both the skill to create such a piece of malware and the desire to target Iranian nuclear facilities.

That said, in many cases the information we described may be forged by nation states or criminals in order to redirect retaliation actions elsewhere or to cover their tracks. Furthermore, in the last few years, a black market has developed, in which hackers offer their services for cyberattacks. In this market, readily available and orchestrated on the Dark Web (a subset of the internet that uses cryptographic protocols in order to maintain the anonymity of users, clients and servers), different actors are selling different services or software tools, which, when assembled, can provide all that is required for performing a cyberattack. These include merchants of corporate emails, credentials, credit cards, exploits, zero-day vulnerabilities, malware and phishing kits designed to provide a user friendly interface for customising and inoculating malware or performing a phishing campaign. The cyberattack supply chain is complex and the information an investigator can gather from the files and the communications used for the attack may be misleading, because it points to different parts of the chain. In these cases, it is important to identify and treat the individual elements of the attack as having possibly originated in different places, in order to avoid misattribution.

Considering the challenges described in this paper, even if a defender recognises the attacker by name, address and phone number, it is often very difficult to prosecute the person. The perpetrator may live in a jurisdiction that is not particularly in alignment with the victim's country. Alternatively, the jurisdiction can be one where the law is difficult to enforce, due to a high level of corruption or where the rule of law is limited. Since, in many of the cases described in this report, the attackers are employed by a government or a criminal organisation, their employer may be actively working to make it difficult to apprehend the perpetrators.



CONCLUSION

Having clarified the different motives behind a cybersecurity-related event, this paper has highlighted the difficulty of distinguishing the different types of cyber threats and the need for clearer distinctions. The aim is that - by gaining a better understanding of the sources of cyberattacks - governments, organisations and individuals will be able to take appropriate steps to manage cybersecurity risks.

But given the novelty of cyberattacks, it is understandable that there is little consensus regarding definitions. When does hacking become espionage and how quickly does this escalate into the use of military force? Indeed, protecting computer networks will not save a country or its citizens from cyberattack, but may even leave it more open to threats. The very same networks will be used by threat actors to deliver their messages and disinformation. Professor Francois Gere of the French Institute of Strategic Analysis says, "If you want to dispatch propaganda and disinformation, you cannot totally disrupt the communications devices of your adversary, so the internet must remain relatively safe and accessible.[4]"

The nature of the threats is changing rapidly, as the main cyber actors change their techniques and strategies. This makes it more, not less, important to understand the source of the risk and the ways in which one cyberattack may differ from another. Only then will governments and organisations be able to bring cyberattacks under control.

[4]https://www.techrepublic.com/article/the-new-art-of-war-how-trolls-hackers-and-spies-are-rewriting-the-rules-of-conflict/

APPENDIX: Timeline of categorised major cybersecurity incidents

TIMELINE OF MAJOR CYBERACTIVISM RELATED INCIDENTS

Year	Name	Description
2017	Spanish government sites	Hackers, allegedly in support of the Catalan independence movement, targeted websites run by Spain's Ministry of Public Works and Transport with DDoS attacks. Some websites were defaced.
2017	Neo-Nazi and KKK websites	DDoS campaign against alt-right and Neo-Nazi groups in the wake of the rally in Charlottesville.
2016	Operation Darknet Relaunch	Hacktivists allegedly linked to Anonymous claimed over 50% of the data stored on the Freedom Hosting II servers contained explicit content. International Business Times reported that the hackers stole 75 GB worth of files and 2.6 GB of databases.
2016	OpOlympicHacking	DDoS campaign targeted various government organisations as a form of protest against hosting the event in Brazil. Different motives were claimed by different sources.
2016	Operation Single Gateway	Hacktivism campaign to protest against the Thai government proposed amendments to the existing Computer Crime Act. Beside the creation of social media content against the Computer Crime Act, several Thai government websites were targeted by DDoS.
2016	Dyn cyberattack	Cyberattack involved multiple distributed DDoS targeting systems operated by Domain Name System (DNS) provider Dyn, which caused major internet platforms and services to be unavailable to a large quantity of users in Europe and North America. The DDoS attack was accomplished through a large number of DNS lookup requests from tens of millions of IP addresses, leveraging the vulnerabilities of many IoT devices.
2015	Operation Comelec	The website of the Philippine Commission on Elections was hacked, allegedly to protest against the low security of vote counting machines. The hacking was followed by a voters' personal information leak. Hackers placed them in the website "wehaveyourdata.com".
2015	Operation KKK (OPKKK)	Different websites allegedly linked to the Ku Klux Klan, a US white-supremacist organisation, were compromised, and a list of 1,000 purported members was publicly posted.

Year	Name	Description
2015	Operation Stop Reclamation	132 Chinese government, educational and commercial websites were defaced or attacked using DDoS, in response to China's reclamation work in territorial disputes in the South China Sea.
2015	Operation CyberPrivacy	Denial of Service attack against Canadian government websites, allegedly in protest of the passage of bill C-51, an anti-terror legislation that grants additional powers to Canadian intelligence agencies. The attack temporarily affected the websites of several federal agencies.
2014	Shooting of Tamir Rice	The website of the US city of Cleveland was attacked using DDoS, allegedly as a protest, after a shooting incident. BeenVerified (an online service to search publicly available information) was used to uncover the phone number and address of a policeman involved in the shooting.
2014	Operation Ferguson	As a protest against a fatal police shooting in Ferguson, Missouri, in the US, a website and a Twitter account were created. The group behind them declared that if any protesters were harassed or harmed, they would attack the city's servers and computers, taking them offline. A DDoS campaign was launched against police websites and connections. A person claiming to be affiliated with Anonymous was releasing information about a policeman, claiming he was the person who carried out the shooting. This was officially denied.
2012	Operation Ababil	DDoS attacks against US banks in retaliation, after a controversial movie was posted on YouTube.
2011-2012	AntiSec Leak and CIA attack	A series of hacking attacks performed by members linked to hacking group LulzSec and GreekSec, the group Anonymous, and others inspired by the announcement of the operation. Information from the Serious Organized Crime Agency, Arizona Department of Public Safety, numerous websites belonging to the Government of Brazil and the energy company Petrobras were released. The CIA's website was taken down for approximately five hours.
2012	Operation Russia	Emails, sent by pro-Kremlin activists and officials, were published.
2012	Operation Syria	As an alleged retaliation against the Syrian government claiming terrorists were disrupting their communication system. Although different claims were circulated about the fact many government sites were hacked, there appeared to be no evidence of this actually happening. The Industrial Bank of Syria's homepage was defaced.

Year	Name	Description
2011	Operation DarkNet	Attackers broke into 40 explicit content websites and published over 1,500 names of users who frequented one of the sites.
2011	Sony data breach	As an alleged retaliation against the publishing of a movie regarding North Korea establishment, an attack was carried out against Sony. Personal details from approximately 77 million accounts were compromised. The data included personal information about Sony Pictures employees and their families, e-mails between employees, information about executive salaries at the company, copies of then-unreleased Sony films, and other information. Sony was forced to turn off the PlayStation Network and to confirm that personally identifiable information from each of the 77 million accounts had been exposed. The outage lasted 23 days, as the perpetrators used specifically designed malware to wipe hard drives, in order to maximise damage and cover traces.
2011	Operation HBGary	A hacking attack against HBGary, a technology security company, was perpetrated after its CEO claimed it infiltrated Anonymous through social networks and was ready to provide information about Anonymous members. The HBGary website was compromised, documents from both HBGary Federal and HBGary, Inc., and emails were publicly posted. The CEO's Twitter account was also taken over.
2011	Operation Egypt	Multiple government websites were shut down using DDoS attacks, and faxes were sent to multiple fax machines in Egypt, allegedly in protest against government attempts to monitor use of the internet in the country.
2011	Operation Tunisia	A series of DDoS attacks were carried out against government websites. Censorship avoidance software was distributed using different channels, in order to provide citizens with the ability to bypass the internet ban.
2011	Attack on Fine Gael website	Data of 2000 people was stolen and sent to the media. The leaked information included IP addresses, mobile phone numbers, e-mail addresses and comments potentially acquired by hacking the website of the political party. The website was then defaced.

TIMELINE OF MAJOR CYBERWARFARE-RELATED EVENTS

Year	Name	Description
2017	Petya	A series of powerful cyberattacks using the Petya ransomware malware affected the internal networks of Ukrainian organisations, including banks, ministries, newspapers and electricity firms. Similar infections were reported in France, Germany, Italy, Poland, Russia, United Kingdom, the United States and Australia. An estimated 80% of all infections were in Ukraine, with Germany second hardest hit with about 9%. Multiple sources agreed that Petya was masquerading as ransomware, while it was actually designed to cause maximum damage, with Ukraine being the main target.
2017	WannaCry	A ransomware malware infected more than 230,000 computers in over 150 countries in 1 day. Parts of the United Kingdom's National Health Service (NHS) were infected, causing it to run some services on an emergency-only basis during the attack, Spain's Telefónica, FedEx and Deutsche Bahn were hit, along with many other countries and companies worldwide. Shortly after the attack began, Marcus Hutchins, a 22-year-old web security researcher from North Devon in England then known as MalwareTech discovered a way to stop the ransomware, which resulted in the infection being halted. New versions designed not to be stopped were since identified in the wild. Multiple sources speculated the attack was only masked as a ransomware and was actually designed to cause large scale disruption.
2016	Interference in the 2016 United States elections	The servers of the Democratic National Committee (DNC) and the personal Google email account of Clinton campaign chairman John Podesta were hacked and their contents forwarded to WikiLeaks. Fake news was circulated, creating fake profiles on multiple social networks and using paid advertisements to boost their reach and target specific segments of population.
2015	BlackEnergy	A malware attack using at least a zero day attack and targeting industrial control systems disrupted many services in Ukraine, including electricity infrastructure, which affected 80,000 customers. The same malware was used to attack airport systems.
2012	Shamoon, also known as W32.DistTrack	Allegedly started with a phishing attack, a unique malware was inoculated into the Saudi Aramco network. Over 30,000 Windows based systems were shut down and their hard drives were wiped. Symantec found some of the affected systems had the image of an American flag whilst data was being deleted and overwritten.
2012	Skywiper/Flamer (Flame)	A modular computer malware targeting Microsoft Windows operating systems was used to attack computer systems in Middle Eastern countries. Probably used for espionage purposes, it spread over a local area network or removable media including over 1,000 machines from private individuals, educational institutions, and government organisations. It also recorded audio, including Skype conversation, keyboard activity, screenshots, and network traffic.
2011	Canadian government hack	The Canadian government was attacked by foreign hackers. These hackers were able to infiltrate three departments within the Canadian government and transmitted classified information out of the country. The government cut off the internet access of the three departments in order to cut off the transmissions while the remediations were happening.
2010	Stuxnet	Stuxnet, a specific malware designed to attack industrial control systems was inoculated in the Middle East, without anyone claiming attribution. The worm allegedly destroyed 1,000 nuclear centrifuges, as it spread beyond the plant and infected over 60,000 computers.
2009	July 2009 cyberattacks	A series of coordinated attacks DDoS against major government, financial websites and news agencies of both the United States and South Korea was executed leveraging a large international botnet.
2008	Election campaign hacking	During the 2008 US presidency run, both candidates systems were hacked, resulting in a big amount of data about their plans, policies and contacts being stolen. Different US government sources were attributing the attacks to governments believed to be acting against the United States.
2007	The government of Estonia hack	A number of techniques, including different types of DDoS attacks were used to take down key Estonian government sites, as a part of a potential government sponsored attack.
2004	Titan Rain	A series of coordinated cyberattacks resulted in hackers being able to infiltrate several computer networks including those at NASA and the Lockheed Martin, Redstone Arsenal, and Sandia National Laboratories. Considered as one of the biggest cyberattacks in history, these acts were allowing access to military intelligence and classified data, and were reported to have left backdoors and persistent threats which could have been used in further attacks.
1982	Trans-Siberian gas pipeline attack	A purported operation sponsored by a foreign government, the Siberian gas pipeline was attacked using a Trojan horse designed to abuse specific code which was managing its control system, resulting in a massive fire. Different sources report the fire as being minor and the consequence of a non-cyber-related incident.

TIMELINE OF MAJOR CYBERCRIME RELATED EVENTS

Year	Name	Description
2017	Equifax data breach	Cybercriminals accessed more than 145 million US Equifax consumers' personal data, including their full names, Social Security numbers, birth dates, addresses, and, in some cases, driver license numbers. Equifax also confirmed at least 209,000 consumers' credit card credentials were taken in the attack. Information on an estimated range of 400,000 to 44 million British residents as well as 8,000 Canadian residents was also compromised.
2017	Grozio Chirurgija cosmetic surgery clinic hack	25,000 digital photos and ID scans relating to patients of the Grozio Chirurgija cosmetic surgery clinic in Lithuania were obtained and published without consent by an unknown group demanding ransoms. Thousands of clients from more than 60 countries were affected.
2017	Orange Is the New Black TV hack	Unreleased episodes posted of Orange Is the New Black TV series online after they failed to extort online entertainment company Netflix.
2016-2017	InterContinental Hotel chain breach	A widespread credit card breach across some 5,000 hotels worldwide owned by InterContinental Hotels Group (IHG). IHG has released data showing that cash registers at more than 1,000 of its properties were compromised with malicious software designed to siphon customer debit and credit card data.
2016	The Bangladesh Bank robbery	Instructions to steal US$951 million from Bangladesh Bank, the central bank of Bangladesh, were issued via the SWIFT network. Five transactions issued by hackers, worth $101 million and withdrawn from a Bangladesh Bank account at the Federal Reserve Bank of New York, succeeded, with $20 million traced to Sri Lanka (since recovered) and $81 million to the Philippines (about $18 million recovered). The New York Fed blocked the remaining thirty transactions, amounting to $850 million, at the request of Bangladesh Bank. It was identified later that Dridex, a specialised malware designed to steal banking credentials, was used for the attack.
2016	Vietnam Airlines	The Check-in systems of VietJet, Vietnam Airlines at the Tan Son Nhat International Airport were attacked and had to stop working. Flight information screens at Noi Bai International Airport were also successfully compromised and posted notices that criticised the Philippines and Vietnam and their claims in the South China Sea. The airlines had to switch to manual check-in procedures leading to 60 flight delays. The official website of Vietnam Airlines was also hacked by the same group at about 4pm the same day. The website page was replaced by the same picture that appeared on the airports' screens. The airlines' customer database was stolen and made public on the internet.
2013-2015	Orchestrated global bank attacks	For a period of two years, ending in early 2015, a group of hackers managed to gain access to secure information from more than 100 financial institutions around the world. The cyber criminals used malware to infiltrate banks' computer systems and gather personal data. They were then able to impersonate online bank staff to authorise fraudulent transfers, and even order ATM machines to dispense cash without a bank card. It was estimated that around $1 billion was stolen from the financial institutions in total.
2015	JP and Morgan Chase & Co	Data related to more than 83 million customers was stolen from JP Morgan. Furthermore, information related to company performance and news was hijacked, which allowed hackers to manipulate stock prices. Using more than 200 fake identity documents, they were able to facilitate large scale payment processing for criminals, an illegal bitcoin exchange, and the laundering of money through approximately 75 accounts globally.
2013	Associated Press' Twitter account's hacks	After successfully gaining access to the Twitter account, the perpetrator posted a hoax tweet about fictitious attacks in the White House that they claimed left President Obama injured. This hoax tweet resulted in a brief plunge of 130 points from the Dow Jones Industrial Average and the temporary suspension of AP's Twitter account.
2014	Yahoo	Data linked to 500 million user accounts was accessed and stolen, including names, phone numbers, passwords and email addresses.
2013	Yahoo	More than one billion user accounts were stolen from Yahoo, including names, phone numbers, passwords and email addresses.
2011	Bank of America hack	An estimated 85,000 credit card numbers and accounts were reported to have been stolen due a cyberattack.
2009	Money Mules	Using specialised malware, hackers stole credentials and executed wire transfers from their accounts. Some of the versions of the malware were rewriting data to prevent the user from being aware of the amounts being transferred.
2008	Heartland	A 2008 attack on Heartland Payment Systems affected an estimated 130 million customers, impacting holders of a variety of credit card types. Heartland eventually paid more than $110 million to Visa, MasterCard, American Express and other card associations to settle claims related to the breach.
2007	TJX	A hacking attack on TJX, a US retailer, affected personal and payment information of at least 94 million customers.

AUTHORS

Simone Vernacchia

Senior Director, CyberSecurity
PwC Middle East

ABOUT PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 158 countries with more than 236,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

Established in the Middle East for 40 years, PwC has 23 offices across 12 countries in the region with around 4,200 people. (www.pwc.com/me).

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

Connect with PwC

www.pwc.com/me

www.twitter.com/PwC_Middle_East

www.linkedin.com/company/pwc-middle-east/

www.worldgovernmentsummit.org