City Preparedness for Cyber-Enabled Terrorism

Report 2022

CTPN
COUNTER TERRORISM
PREPAREDNESS NETWORK

Lead Authors

Jakob Bund
Project Lead Cyberdefense and Senior Researcher
Center for Security Studies, ETH Zürich

Alice Crelier
Cyberdefense Researcher
Center for Security Studies, ETH Zürich

David Peri
Cyber Threat Intelligence Analyst
Homeland Security and Emergency Management Agency
Washington DC

John Pfautz
Cyber Threat Intelligence Analyst
Homeland Security and Emergency Management Agency
Washington DC

Stefan Soesanto
Senior Cyberdefense Researcher
Center for Security Studies, ETH Zürich

Sebastian Tabrizzi
Security Strategist
City of Stockholm

Alex Townsend-Drake
Head of Programme
Counter Terrorism Preparedness Network

Lead Reviewer
Akvile Giniotiene
Head of Cyber and New Technologies Unit
United Nations Counter-Terrorism Centre (UNCCT)
United Nations Office of Counter-Terrorism (UNOCT)

Independent Reviewers

Inspector Dean Akinola and Chief Inspector Andy Burton
Counter Terrorism Security Coordinators
Metropolitan Police Service

Toby Gould
Deputy Head of London Resilience
Capabilities and Response Operations
London Resilience Group

Kenn Kern
Chief Information Officer
Special Assistant for International Relations
New York County District Attorney's Office

Janette Palm
Cyber Security Strategist
City of Stockholm

Dr Gianluca Pescaroli
Director of the MSc in Risk, Disaster and Resilience
Institute for Risk and Disaster Reduction
University College London

Dr Magnus Ranstorp
Strategic Advisor
Center for Societal Security
Swedish Defence University

Eneken Tikk
Executive Producer
Cyber Policy Institute

Anonymised Reviewer
Counter Terrorism and Cybercrime Centre
European Union Agency for Law Enforcement Cooperation (Europol)

Expert Members
Counter Terrorism Special Interest Group
The Security Institute

1 Overview and Context

“Terrorist groups may eventually acquire the capacity to launch terrorist attacks through the Internet, thereby causing damage to critical infrastructure, industrial control systems, or Internet of Things (IoT) devices.”

United Nations
‘Information and Communications Technologies Factsheet’

Executive summary

Cyber-threat actors include states, serious organised crime groups and other non-state actors such as terrorists. The need to be prepared for terrorists seeking to take advantage of societies’ increasing cyber-dependencies has been recognised by the UN Security Council through Resolution 2341 (2017). This calls upon Member States to collect and preserve digital evidence to hold to account those responsible for terrorist attacks and to address the exploitation of information communication technology (ICT) by terrorists.[1] It noted how critical infrastructure protection against terrorist attacks requires the convergence of multiple efforts including cyber-security.[2] The UN Office for Disarmament Affairs also convenes governmental experts on developments in the field of information and telecommunications in the context of international security.[3]

> **“Without action it is increasingly clear that the key technologies on which we will rely for our future prosperity and security won’t be shaped and controlled by the West. We are now facing a moment of reckoning.”**

The UN highlighted that “terrorist groups may eventually acquire the capacity to launch terrorist attacks through the Internet, thereby causing damage to critical infrastructure, industrial control systems, or Internet of Things (IoT) devices”.[4] The international community recognises and prioritises these issues through the Global Counter-Terrorism programme on Cybersecurity and New Technologies, as implemented by the UN Office of Counter-Terrorism. This serves as an instrument to support Member States in strengthening their capacities to develop and implement an effective response to this emerging threat.[5] This position provides the backbone for this report. Although cyber-enabled terrorism has not yet risen (because of the technical capability needed to mount a successful attack), it is considered a credible threat.

This report supports the drive to further protect critical infrastructure (which may reside in and is central to city operations) from cyber-attacks and, by extension, cyber-enabled terrorism. To do so, it focuses on preparedness for critical infrastructure, essential services and city operations, arguing that societies’ dependence on, and the interdependence between, digital infrastructure offers potential avenues for cyber-enabled terrorism.

By doing so, this report aims to engage authorities (specifically those at a city level) by providing evidence of the need to continually enhance preparedness against a range of cyber-threats and work to ensure that the frequency and severity of cyber-enabled terrorism doesn’t increase.

Note that this report does not provide a threat assessment. It does not intend to take a position on the threat or likelihood of cyber-enabled terrorism, and thus probabilistic language is kept to a minimum. Indeed, it is acknowledged that terrorists are currently considered to be low-capability actors in this regard. Rather, this report recognises that the threat exists, as does the ability for it to be discharged through crime-as-a-service platforms, and thus there is a need for cities, in general, to improve preparedness for cyber-attacks.[6] The need to enhance preparedness for cyber-attacks, and those with real-world implications, is the key message.

Currently, there are an estimated 8.6 billion internet-based connections globally, a figure that is projected to almost triple by 2026 to 23.6 billion.[7] As technology's ability to transmit, collect and store data matures, it will create additional attack vectors for hostile actors, including terrorists, to exploit.[8] This will become increasingly challenging as more people, devices, systems and processes become connected.

A recent report, *'Why Cyber Resilience Must Be a Top-Level Leadership Priority'*, stated, "our societies rest upon a digital foundation every bit as critical as our transportation, health, electricity, water, and sewage systems".[9] Indeed, this very digital foundation enables these critical services to operate.

Understanding this level of dependency opens a window into the potential challenges presented by cyber-attacks. Mapping vulnerabilities and consequences then taking a foresight-based approach towards emerging threats means that implications for city preparedness can be considered. This is an important step in translating security strategy into practice at a city level, developing robust multi-agency arrangements and building both preparedness and resilience in a holistic and intelligent way. Taking a holistic and integrated approach towards driving city preparedness, security and development is a core principle of the Counter Terrorism Preparedness Network that translates to the cyber-threats faced.

A sustainable strategy and systematic approach towards securing and future-proofing cyber-based systems that drive city operations is crucial and has never been more pressing. Herein lies the delicate balance between harnessing the benefits of cyberspace and technology versus ensuring security and preparedness against exploitative acts. This need to converge cyber- and physical security is an evolution in our collective journey.[10] GCHQ Chief Jeremy Fleming underscored this when he said, "without action it is increasingly clear that the key technologies on which we will rely for our future prosperity and security won't be shaped and controlled by the West. We are now facing a moment of reckoning".[11]

This report:

1. Seeks to understand the current landscape of cyber-attacks
2. Explores the contested concept of cyber-terrorism and frames "cyber-enabled terrorism"
3. Analyses system vulnerabilities relating to critical infrastructure and essential services, and the potential consequences for cities, incorporating transferrable case studies to integrate learning
4. Predicts emerging threats related to cyberspace and artificial intelligence (AI)
5. Proposes measures to enhance preparedness and resilience

Primary focus

Global strategic trends are pushing cities towards a significantly more automated world that fuses the physical, digital and biological.[12] This dependence on cyberspace, AI and rapidly advancing technologies can harm society if used for malicious ends by hostile actors.

> **This intangible space will become increasingly challenging as more people, devices, systems and processes become connected. This is exacerbated by the complexities of cities, which hold a high degree of digital dependence to maintain and deliver vital societal functions.**

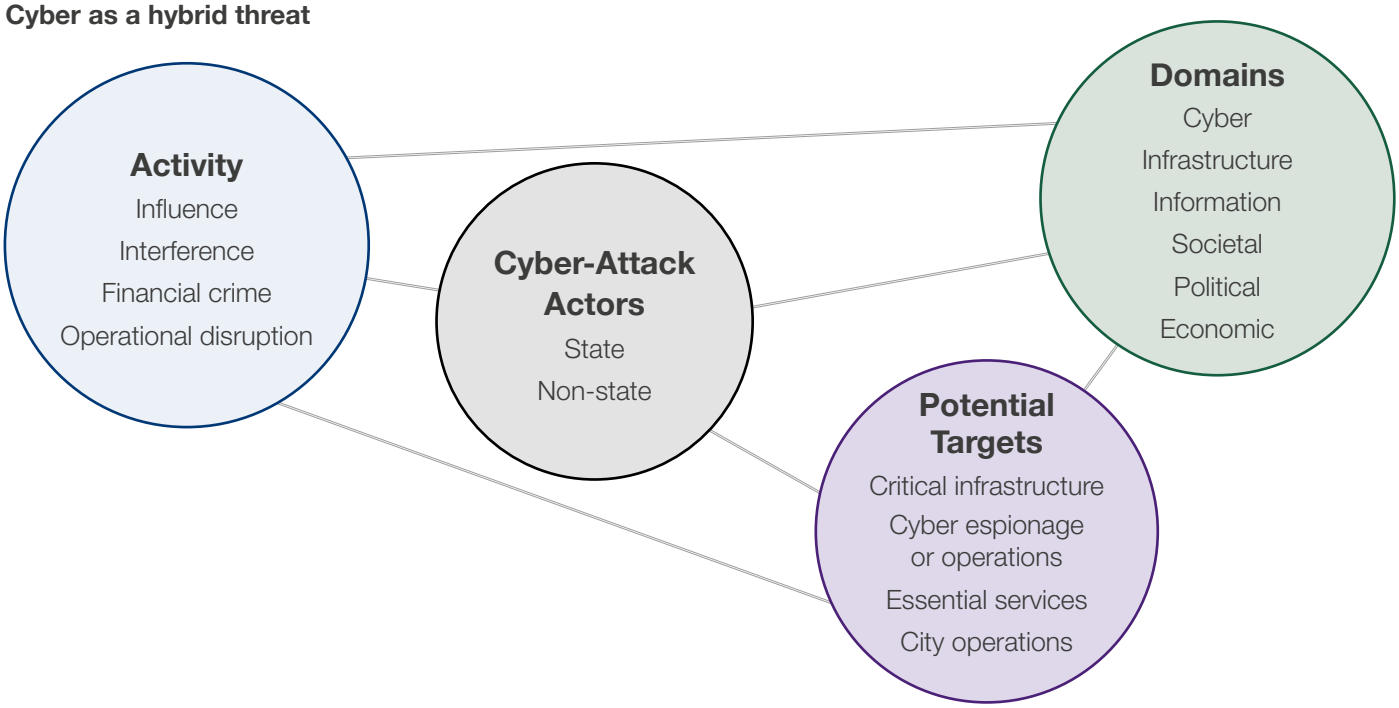
The UN Secretary-General's Strategy on New Technologies acknowledged both the great promise and risks that these new technologies bring. It noted that "While cyberspace has come to underpin almost every aspect of our daily lives, the scale and pervasiveness of 'cyber insecurity' is also now recognised as a major concern. The political and technical difficulty of attributing and assigning responsibility for cyber-attacks encourages actors to adopt an offensive posture, not only amongst states but also from non-state armed and criminal groups and individuals seeking to develop or access potentially destabilising capabilities with a high degree of impunity."[13]

Cyberspace, and increasingly AI, has become the foundation of everyday technologies. Cyberspace can be defined as a "complex environment resulting from the interaction of people, software and services on the internet by means of technology devices and networks connected to it, which does not exist in any physical form".[14] This intangible space will become increasingly challenging as more people, devices, systems and processes become connected. This is exacerbated by the complexities of cities, which hold a high degree of digital dependence to maintain and deliver vital societal functions.

Attacks against the internet or devices, networks and services or systems connected to it have the potential to be high-consequence in this setting.

In a world where low-level cyber-crime has become the norm, anyone with access to computer systems or mobile devices will be aware of the phishing scams, ransomware and malware that bombard users daily. This is a view endorsed by Interpol, which highlighted how cyber-crime is progressing at an incredibly fast pace, with complex criminal networks operating across the world and coordinating intricate attacks that can be executed in a matter of minutes.[15] In July 2021, Interpol Secretary General Jürgen Stock called for immediate action to avoid a ransomware pandemic.[16] Indeed, the cyber-threat is becoming much greater and will continue to grow.[17]

Cyber as a hybrid threat



"Cyberspace provides a new delivery mechanism that can increase the speed, diffusion, and power of an attack, and ensure anonymity and undetectability. The low price of entry, anonymity, and asymmetries in vulnerability mean that smaller actors have more capacity to exercise power in cyberspace than in many more traditional domains of world politics".[19]

There are indications that we are approaching a tipping point that will lead hostile actors towards this more unconventional mode of attack,[18] an instrument of hybrid warfare that falls in the area between peace and conflict utilised by both state and non-state actors, termed the grey zone.

The European Commission report *'The Landscape of Hybrid Threats: A Conceptual Model'* explores the different domains of hybrid threats including cyber. It highlights that anything of significance in the real world also takes place in cyberspace and therefore the cyber dimension plays an exceptional role. The report is explicit in its statement that "cyberspace provides a new delivery mechanism that can increase the speed, diffusion, and power of an attack, and ensure anonymity and undetectability.The low price of entry, anonymity, and asymmetries in vulnerability mean that smaller actors have more capacity to exercise power in cyberspace than in many more traditional domains of world politics".[19]

Sophisticated actors are now prepared to devote significant time and resources towards achieving strategic advantages in cyberspace, with spending on cyber-security projected to rise exponentially.[20]

"This unprecedented fusion between politics, strategic manoeuvre, commerce, and crime is beginning to pose unique challenges".[21] As the UK Security Service warned, these less visible threats have the potential to affect us all, including our jobs and public services – even leading to a loss of life.[22]

Cyber-attacks could be employed as a tactic by any number of hostile actors. Although states are known to have the highest levels of offensive cyber-capabilities, non-state actors are thought to carry out the majority of cyber-attacks, whether for themselves or for a state that does not want to disclose its sponsorship.[23] However, the likelihood that terrorists in particular will develop their ability to organise and implement cyber-attacks remains unclear and open to debate. At this time, terrorists are considered to be low-capability actors. Yet, as this report will note, terrorist groups have expressed their intent.

Terminology and framing

A cyber-threat can be understood as any circumstance or event with the potential to adversely impact organisational operations, assets or individuals through unauthorised access to systems for the destruction, disclosure and modification of information, and/or denial of service.[24] In this respect, the potential for cyber-enabled terrorist attacks against critical infrastructure is of interest.[25]

In this context, the definition of a cyber-attack as targeting the "use of cyberspace for the purpose of disrupting, disabling, destroying or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information"[26] applies. It could also be understood as an event or situation caused by, or causing, a failure of electronic ICT systems that threatens serious damage to human welfare, the environment, the effective delivery of critical public services or to security.[27]

Therefore, a cyber-attack, in the context of this report, specifically refers to intentional, unlawful and significant attacks that infiltrate, exploit and/or impact upon or deny critical infrastructure, essential services and city operations with real-world implications (regardless of the initiating actor).

Looking at cyber-attacks from a range of actors allows for a variety of examples to be drawn upon and considered when applied in the context of terrorism.

Indeed, views differ on the likelihood and impact of cyber-enabled terrorism, the associated terminology and the ways in which the subject is framed. One of the main blockers is the challenge of attributing responsibility for cyber-attacks and the lack of clear classifications. For this reason, this report refers to transferrable case studies and risk-based scenarios through the lens of cyber-enabled terrorism. This approach and choice of terminology is rationalised below.

Concept of cyber-terrorism

The term "cyber-terrorism" was coined in the late 1980s to explain the phenomenon that includes both terrorism and cyberspace.[28] In the context of the bombing of the World Trade Center in 1993, the Oklahoma Bombing in 1997 and the bombings of the US embassies in Kenya and Tanzania in 1998, cyberspace was seen as a potential vector to reach connected societies. Against this backdrop, the Naval Postgraduate School published a white paper called *'Cyberterror: Prospects and Implications'* in 1999,[29] which was the first comprehensive study to address the issue of cyber-terrorism.[30]

In contrast to conventional terrorist attacks, cyber-terrorism did not necessarily threaten violence against people or physical structures. Rather, these attacks could be operations that sought to disrupt or destroy digital property.[31] The geopolitical context at the end of the 20th century, as well as the beginning of digitalisation and the debates around the "information society", further catalysed the emergence of cyber-terrorism as a concept.

A cyber-attack, in the context of this report, specifically refers to intentional, unlawful and significant attacks that infiltrate, exploit and/or impact upon or deny critical infrastructure, essential services and city operations with real-world implications.

Shortly after the 9/11 terrorist attack against the US, a hacking group called the Dispatchers announced it would target nations that supported terrorists. It defaced hundreds of websites and launched Distributed Denial-of-Service (DDoS) attacks against targets including the Iranian Ministry of Interior and the presidential palace in Afghanistan,[32] to showcase the potential impact of their capabilities.

Three years later a further publication, *'Terrorism in the Information Age: New Frontiers'*,[33] highlighted the vulnerability of critical infrastructure to attacks and demonstrated terrorists' interest in targeting such sites.

More recently, the concept of cyber-terrorism has been the focus of renewed interest from academia, news organisations, government bodies and the international community, especially in light of the recent wave of ransomware attacks targeting or affecting critical infrastructure operators, such as hospitals in France and Ireland, and pipeline systems and meat-processing plants in the US.[34]

These showed how attacks on data, digitally dependent systems or operations could manifest with real-world implications.

However, one of the main controversies concerning cyber-terrorism revolves around the definition and delimitation of the concept.[35]

Drawing on the field of terrorism studies more broadly, proposed sets of defining characteristics include violence or the threat thereof; pursuit of a political goal; intent to produce fear; messaging to multiple audiences (including to the target and the attackers' supporters); exercise of power that is embedded in a broader political struggle and an expression of warfare.[36] The lack of evidence pointing to cyber-terrorism has compounded this issue.[37]

In the absence of a recognised set of case studies, research on the potential of cyber-terrorism has necessarily referred to examples that "are either cases of hacktivism, cyber-crime, or nation-state operations".[38]

Yet, "the continuing popularity of cyber-terrorism as a concept – and fear – has been underpinned by established economic and political interests, as much as by psychological fears of its occurrence".[39] International discussions about cyber-terrorism have been constrained by concerns about the possible misappropriation of the term to garner international support for the repression of domestic political opposition under the label of combating terrorism.

Drafts of an International Code of Conduct for Information Security have invited particular scrutiny of the definition and use of the term.[40] This called for cooperation in combating terrorist activities that use ICT in the context of vaguely identified activities that undermine "political, economic and social stability" and subvert the "spiritual and cultural environment".

> **The concept of cyber-terrorism remains problematic politically but also operationally, when it can be difficult to distinguish from other cyber-crimes.**

Indeed, studies show that cyber-terrorism is not clearly defined under international law, and that even if at the national level a large majority of countries' laws refer to cyber-terrorism, they do not distinguish it from other terrorist tactics.[41,42]

This remains a challenge and raises the question whether cyber-terrorism should be distinct or included within a broader understanding of terrorism as one of many tactics.

In 2021, the UN General Assembly endorsed the need to advance responsible state behaviour in the use of ICTs, holding discussions on the topic at the UN level that were open to all Member States and to input from non-governmental stakeholders.

These consultations serve as important progress and boosts political momentum for a more collaborative, multilateral approach. However, the position is not yet advanced enough to offer a starting block for the analysis of an internationally shared definition.

The concept of cyber-terrorism remains problematic politically but also operationally, when it can be difficult to distinguish from other cyber-crimes.

It is no surprise that research on cyber-terrorism in the context of cities is scarce. A paper on cyber-warfare and social disorder, for instance, does not explicitly mention the term in the analysis but does address cyber-warfare in the context of cities by drawing on a foresight scenario.[43]

Another openly deals with cyber-terrorism (without trying to define it) in the context of smart cities.[44] Today, most of the cities that could fall victim to cyber-terrorism are already so connected and dependent on technology that it is realistic to say that they qualify as "smart cities".

For this reason, this report makes no conceptual distinction between cities and smart cities. Instead, it looks at factors in a city context that might be vulnerable to cyber-terrorism or what may be better understood as "cyber-enabled terrorism".

Cyber-enabled terrorism

Due to the challenges identified in defining and attributing responsibility for cyber-terrorism, this report introduces the term "cyber-enabled terrorism". The proposal is that cyberspace serves as an enabler for terrorism. That is not to make any claims or judgments on threat, likelihood and capability, but rather to acknowledge the capacity of cyber-attacks to drastically expand the reach of terrorist groups. The means to deliver such an attack may take advantage of shared system vulnerabilities to harm numerous targets in different locations – possibly even inadvertently – highlighting the importance of preparedness efforts.

This lens refines the focus of the report to consider the potential vectors for, and impacts of, cyber-enabled terrorism. It will draw upon broad examples of significant cyber-attacks by hostile actors to support a consequence-based analysis to develop understanding of the real-world implications for critical infrastructure, essential services and city operations.

The rise in and consequences of cyber-attacks – notably the recent spate of ransomware attacks – show that the risk is heightened by society's dependence upon, and interdependence with, cyber-based systems.

Broadly reflect how, in 2015, telecommunications provider TalkTalk reported a data breach that leaked approximately 157,000 customer records, a breach that was accompanied by an email to employees with a ransom demand.[45] In 2017, the WannaCry attack tore across the globe and took down parts of the UK's National Health Service (NHS). This same year, a "Freedom of Information request sent to UK Critical National Infrastructure found that over a third of their IT outages were caused by cyber-attacks".[46]

Fast-forward and the year 2020 broke all records when it came to the sheer numbers of ransomware attacks and data lost in breaches.[47]

In 2021, an attack took down a pipeline supplying half the fuel to America's east coast;[48] another attack attempted to poison the water supply of a city in Florida by remotely increasing the amount of sodium hydroxide;[49] and Coop Sweden closed 665 stores after point-of-sale tills and self-service checkouts stopped working due to software infiltration, thus halting the sale of food.[50]

The latter was, of course, a small part of a much larger global supply-chain attack against a major service provider that further underscores the national security dimension of the cyber-threat.[51]

A list of "significant" cyber-attacks (that is those against government agencies, defence and high-tech companies or economic crimes with losses of more than a million dollars) is maintained by the Centre for Strategic and International Studies.[52]

This demonstrates a staggering upward trend, with well over 100 attacks that meet their "significant" threshold in 2021 alone. The European Union Agency for Cybersecurity offers a deeper analysis of the main cyber-attacks experienced and their origins.[53] When all is considered, it is unsurprising that mainstream media refer to "the age of the cyber-attack".[54]

Cyberspace serves as an enabler for terrorism. That is not to make any claims or judgments on threat, likelihood and capability, but rather to acknowledge the capacity of cyber-attacks to drastically expand the reach of terrorist groups.

These trends have driven the US Department of Justice to raise the priority of its ransomware investigations to the level assigned to terrorism.[55] This perception of ransomware attacks, even when carried out by criminal groups, indicates the gravity with which they are viewed and the impact they can have. Whether a cyber-attack is international, national or local in scale; targeted (individual, organisational or regional); or widespread (organic and sporadic based on software or systems etc.), it can have significant consequences that play out at all levels of society.

This is evident to hostile actors, including terrorists, who may see cyberspace as an enabler for facilitating campaigns and attacks.

Indeed, cyberspace – the internet, dark web, social media and end-to-end encrypted messaging – has already provided powerful tools for terrorist groups.[56,57]

The dark web, for example, offers anonymous and deniable means for malicious actors to converge and can serve as a forum for conversation, coordination and action between them.[64] It can facilitate transnational exchanges between hostile groups, enable access to countless forms of illicit products and criminal services.

ISIS is known to have hacked into dormant Twitter accounts,[58] for example, and numerous investigations and counter terrorism operations have shown the use of encryption by Al-Qaeda and ISIS-affiliated individuals, enabling them to communicate more quickly and covertly over expanding distances to foster terror faster and at a larger scale.[59]

Recruitment, radicalisation, fundraising, the dissemination of propaganda and the encouragement of violence or facilitation of physical attacks are all driven through online channels.[60,61] In one example, four fake websites from known Islamist extremist groups were using crypto-currency funds to support terrorist operations.[62,63]

This exploitative mindset is combined with generational shifts in cyber-expertise and training; underworld platforms on the dark web that transcend borders; clandestine networks; and a micro-economy built upon crypto-currencies.

The dark web, for example, offers anonymous and deniable means for malicious actors to converge and can serve as a forum for conversation, coordination and action between them.[64] It can facilitate transnational exchanges between hostile groups, enable access to countless forms of illicit products and criminal services, as well as provide an avenue for propaganda and targeting of the vulnerable.

The opportunities offered by this remote and largely untraceable space embody the very principle of cyber as a tool for malicious intent. There is a sliding scale, from terrorists using ICT for operational or other purposes all the way to terrorists that may seek to exploit cyber-technologies to attack digital, virtual or physical targets. Academic inquiry into this space is still in its infancy[65] but terrorists could benefit from cyber-dependencies and emerging technologies, which tend to be under-regulated and under-governed.[66]

In 2012, in the wake of a video message by Al-Qaeda calling on its followers to carry out cyber-attacks, the then US Assistant Attorney General Lisa Monaco voiced the belief that "it is a question of when, not if, they will attempt to do so".[67]

Between late 2016 and early 2017, ISIS launched its first-ever successful series of DDoS attacks, coordinated via a top-tier ISIS dark web forum and targeting mainly government infrastructure. It was reported that ISIS had used a DDoS-for-hire service, showing the link between cyber-crime and cyber-enabled terrorism.[68]

The advent of the crime-as-a-service model, whereby the tools of the cyber-crime trade can be used for fundraising or sold for a monetary value, creates the concern that it may be possible for low-skilled terrorist groups to simply purchase services and pre-built or custom-made algorithms. The European Cybercrime Centre now offers expertise for investigations where cyber-crime and terrorism converge.[69]

Since 2017, the ISIS hacking division has *claimed* (note: challenges in assessing the credibility of claims is a barrier in understanding the origin of cyber-attacks) responsibility for attacks disrupting online services[70] and Europol has reported further calls from terrorist groups to use cyber-attacks against sensitive targets.[71]

Cyberspace has been used maliciously by terrorists; it can also serve as a vector for terrorist attacks as well as a direct enabler for the facilitation of cyber-attacks. Cyber-enabled terrorism has the potential to spread fear, intimidate populations or compel a government or international organisation to do (or to abstain from) any act.

The number of examples and scenarios of cyber-attacks demonstrate how DDoS attacks, ransomware Campaigns, phishing, data manipulation and the defacement of websites could be attractive to terrorists.

These could be carried out on targets such as emergency or public services (including water, power, telecommunications, healthcare or transport infrastructure/ networks), supermarkets, banks and businesses, as well as supply chains and logistics. The fact that cyberspace is at the heart of modern society and impacts life in so many ways has driven aggressive approaches from governments to confront cyber-threats.[72,73,74,75]

The UK levels for cyber-incidents[76] are used in the London Cyber Incident Response Framework,[77] which aids understanding by distilling significant cyber-attacks into three categories:

All three categories are relevant to this report, but notably categories one and two. This is because although category one is classed as a national cyber-emergency, it may well be focused in a city or cities, and/or affect a range of cities. Notably, this type of attack would differ from the usual terrorist modus operandi. It may be protracted and cascade, slowly or quickly, well beyond the frames of normal continuity planning.

The next section draws upon real cases of non-terrorist cyber-attacks that are otherwise transferrable in assisting understanding of the vulnerabilities and interdependencies in systems and services that can be exploited.

1. **National Cyber Emergency:**
A cyber-attack that causes sustained disruption of essential services or affects national security, leading to severe economic or social consequences or to loss of life.

2. **Highly Significant Incident:**
A cyber-attack that has a serious impact on central government, essential services, a large proportion of the population or the economy.

3. **Significant Incident**:
A cyber-attack that has a serious impact on a large organisation or on wider/local government or poses a considerable risk to central government or essential services.

The advent of the crime-as-a-service model, whereby the tools of the cyber-crime trade can be used for fundraising or sold for a monetary value, creates the concern that it may be possible for low-skilled terrorist groups to simply purchase services and pre-built or custom-made algorithms.

2 Vulnerabilities and Interdependencies

> **“Cyber-infrastructure underpins critical infrastructure such as power plants, water and wastewater facilities, hospitals, telecommunications systems, oil and gas refineries and transport networks.”**
>
> US Cybersecurity and Infrastructure Security Agency *‘Infrastructure Resilience Planning Framework’*

In 2021, the US Cybersecurity and Infrastructure Security Agency released an Infrastructure Resilience Planning Framework. It highlighted the need to understand society’s reliance on ICT systems to operate and monitor critical infrastructure and to support key social and economic functions, such as the provision of essential public services. This is important because cyber-infrastructure underpins critical infrastructure such as power plants, water and wastewater facilities, hospitals, telecommunications systems, oil and gas refineries and transport networks.[78] An attack against these would pose direct security threats.

To explore this further, this section examines a range of cyber-attacks that have had real-world impact. It seeks to outline lessons learned from real cases that can be viewed through the lens of cyber-enabled terrorism and applied to inform preparedness. Although the cases used are not classified as terrorism, they offer transferrable examples that demonstrate the digital dependence of society, notably critical infra-structure and services, enabling a fuller understanding of the potential effects of cyber-attacks.

The analysis starts by exploring known impacts of attacks on critical infrastructure and essential services, before looking at the associated challenges posed by data exfiltration and destruction. It touches upon the psychological impacts of cyber-attacks before concluding with a system view of vulnerabilities.

Critical infrastructure

Cyber-attacks on critical infrastructure can cause second- and third-order effects that cascade through city systems and probably cause more collateral damage than the actual cyber-attack itself. The ransomware campaign against Colonial Pipeline in May 2021 hit the company’s business IT systems rather than the operational end that controls pipeline flows, pressure and other metrics. However, as information on payments, order flows and inventory storage was probably inaccessible and Colonial needed to contain, isolate and fully assess the threat, the company decided to take certain systems offline, including the main pipelines.[79] This decision resonated through the US ecosystem and led to delivery disruptions, panic buying and thousands of petrol stations down the East Coast running out of fuel.[80] Societies’ demand for fuel means that such destabilisation can have far-reaching effects on the functioning of cities, supply chains, the economy and even international politics.

Other effects were at play when a ransomware campaign was run against the Düsseldorf University Hospital in Germany in September 2020. The ransomware infected the hospital’s IT system that was used to coordinate doctors, treatments and bed occupancy. As this data was inaccessible, the hospital had to cancel thousands of operations, drastically limit its capacity to treat patients and stop all new admissions.

Cyber-attacks on critical infrastructure can cause second- and third-order effects that cascade through city systems and probably cause more collateral damage than the actual cyber-attack itself.

The effective closure of the hospital also led to the redirection and eventual death of a 78-year-old woman with an aortic aneurysm. After a two-month investigation, the public prosecutor concluded that a) the delay was of no relevance to the final outcome; b) that the medical condition was the sole cause of the death; and c) that this was entirely independent from the ransomware attack.[81]

The Chief Public Prosecutor responsible for the investigation, however, pointed to the case as "a warning sign to those running critical infrastructure" that failure to adequately protect these systems "could result in fatal outcomes".[82] Indeed, cyber-attacks on healthcare can have serious consequences, as demonstrated by the WannaCry attack that impacted the UK's NHS.

CASE STUDY
WannaCry ransomware attack

On Friday 12 May 2017, a global ransomware attack known as WannaCry affected a wide range of countries and sectors. WannaCry infected computers running certain versions of the Microsoft Windows operating system by exploiting a specific Windows vulnerability, encrypting data and demanding ransom payments in the Bitcoin crypto–currency. Within one day, it was reported by Europol to have infected more than 250,000 computers in at least 150 countries,[83,84] including systems within the NHS.

This case study will outline the NHS response, the impact upon the NHS and lessons identified throughout the incident. The attack affected at least 80 out of the 236 NHS trusts across England, either because some computers were infected by the ransomware or devices were turned off as a precaution. A further 603 primary care and other NHS organisations were also infected, including 595 doctors' surgeries.[85]

The cyber-security firm Avast identified WannaCry as one of the broadest and most damaging cyber-attacks in history.[86] As well as being the largest cyber-attack to affect the NHS to date, WannaCry's impact was recorded as far afield as Russia, Ukraine and Taiwan, with Chinese universities, Spanish Telefónica and global firms including FedEx, Nissan and Renault also affected.[87]

NHS response

NHS Digital's CareCERT service alerted the Department of Health (DH) at approximately 13.00 on 12 May 2017, following reports from multiple NHS trusts. The attack was designated as a major incident by NHS England at 16.00, warranting implementation of a national command and control structure under existing Emergency, Preparedness, Resilience and Response plans.

NHS England acted as the single point of coordination for incident management with support from NHS Digital and NHS Improvement.

Over the course of the day, the incident-management activities gained pace. From 17.00, regional incident coordination centres in NHS England began to seek assurance from local NHS organisations that action was being taken in line with the CareCERT communications. Local organisations worked to resolve and prevent infection where possible. Later in the evening of 12 May 2017, a UK malware researcher discovered a "kill switch" that stopped the malware from spreading further.

NHS Digital wrote to all trusts on 14 May 2017 advising against the payment of ransoms, and according to DH, NHS England and the National Crime Agency, no NHS organisation paid the requested ransom.[88] The NHS response to the attack was shaped by three phases:

- Protecting the emergency care pathway
- Assuring primary care was operationally stable
- Remediation patching, wider system actions and applying the anti-virus update

In accordance with existing plans for major incident response, NHS England initially focused on maintaining emergency care services. The timing of the attack, starting on a Friday, resulted in minimal disruption to primary care services, which are usually closed over the weekend. Over the weekend, 20 of the 25 infected acute trusts

continued to treat urgent and emergency patients. However, five trusts had to divert patients to other emergency departments, and a smaller number needed further outside help to continue treating patients. By 16 May 2017, fewer than five hospitals were still diverting patients[89] and several other trusts had problems with key diagnostic services.

The WannaCry attack disrupted NHS services across the country until 19 May 2017, when the national incident was stood down. During this period, DH and NHS England worked with NHS Digital, NHS Improvement, the National Cyber Security Centre, the National Crime Agency and others to respond to the attack and to support NHS services in providing care to patients.

NHS England implemented major incident plans and coordinated the response through the same teams and structures that would deal with any other national major incident. This was a robust framework through which to manage the incident. Lessons were subsequently identified about how the management of a cyber-attack differs from other types of major incidents.

Impact and lessons

Healthcare is a complex environment with many connected systems. The NHS responded effectively to this major incident, with no reports of harm to patients or of patient data being compromised or stolen. It is estimated by NHS England that 1% of NHS activity was directly affected by the WannaCry attack over the week of the attack. Out of 236 hospital trusts across England, 80 were affected, where services were impacted even if the organisation was not infected by the virus (for example, if they chose to take email servers or network connections offline to reduce the risk of infection).

Some critical medical devices and equipment were still using unpatched Microsoft Windows 7 or XP software supplied by third parties and were affected including, for example, Magnetic Resonance Imaging (MRI) scanners and blood-test analysis devices. The result was that normally functioning diagnostic devices were rendered unusable as the software was running on an infected device and needed to be patched or quarantined. NHS England identified that 6,912 appointments had been cancelled and estimated that more than 19,000 appointments would have been cancelled in total, based on the normal rate of follow-up appointments.

It is not known how many doctor appointments were cancelled, or how many ambulances and patients were diverted from the five emergency departments that were unable to treat some patients. NHS England says that it is not possible to calculate with certainty the financial impact of the WannaCry attack. One estimate places the overall costs to the NHS at £92 million, including lost output and IT costs from the attack.[90]

In the aftermath of the WannaCry cyber-attack, an extensive programme of single- and multi-agency debriefs and after-action reviews were undertaken. The DH Data Security Leadership Board also commissioned the Chief Information Officer for the health and social care system in England to carry out a comprehensive review of the attack. The National Audit Office also investigated the effect the WannaCry attack had on the NHS in England.

The recommendations from these reviews and implementation of lessons were tracked through a series of reports that proceeded into 2019, as summarised below.

The review by the Chief Information Officer concluded that the attack highlighted vulnerabilities within the NHS in England. It exposed a need to improve across the NHS, including discipline and accountability around cyber-security at senior leadership and board level, and the importance of swift and effective patching of systems when new security updates are released. The review also highlighted historic under-investment in network security and up-to-date software.

CASE STUDY
WannaCry ransomware attack (continued)

One of the key lessons was the need for clarity on leadership and accountability for any future cyber-security incidents. This was addressed through the development of a "cyber handbook" to describe the approach and actions to be taken by NHS England, NHS Improvement and NHS Digital in the event of a cyber-attack. In principle, DH would lead, with NHS England coordinating the system response.

The review recommended the development of local organisation business-continuity, cyber-response and disaster-recovery plans to include the necessary detail around cyber-incidents. This included the assessment of the impact of the loss of services on other parts of the health and social care system.[91]

It also highlighted that plans should be regularly tested across local organisations and partners, with board-level oversight. NHS Digital has produced a Cyber Incident Response Exercise[92] to support local organisations in testing incident response in health and social care.

The need to build the resilience of local organisations was further driven by recommendations to develop provider and digital services; protect patient pathways; remove or isolate unsupported systems and unpatched versions of software; and to invest in infrastructure. Recommendations to enhance local infrastructure and planning were coupled with developing more robust governance arrangements. This meant that all NHS organisations are now required to appoint an executive director as data security lead; cyber-security risks must be regularly reviewed by the board; and appropriate counter-measures are to be in place to mitigate or reduce the impacts of a successful attack while addressing service restoration.[93]

There has been a drive to lead on digital transformation across the NHS, embedding responsibilities for providing strategic direction for, and monitoring, cyber-security. Significant work was also undertaken to develop the NHS Digital CareCERT system, which has now evolved into the "Respond to an NHS cyber alert" system, which allows messages to be sent to health and social care organisations, provides confirmation of receipt and receives updates on progress with remediation work.

It is inevitable that health and social care systems will face attacks in the future. This requires vigilance and a process of evaluating and appropriately managing these threats. As such, the DH and NHS continue to invest in cyber-security at all levels. As the threat landscape continually evolves and digital systems become more and more entrenched in the delivery of healthcare to the public, there have been improvements in three key areas: cyber-monitoring, threat intelligence and incident response; support and guidance for local organisations; plus cyber-training, awareness and engagement with cyber-security best practice.

Case study courtesy of NHS England (London), as provided by Barry Emerson, NHS Specialist Advisor to London Resilience and Dr Chloe Sellwood, Deputy Head of Emergency Preparedness, Resilience and Response.

Cyber-attacks on health and social care systems have the potential to be high-impact and high-consequence. Although the risk of cyber-attacks on healthcare as a result of cyber-crime is very real, the risk of it happening as a result of cyber-enabled terrorism is considered unlikely. The context of cyber-enabled terrorism should, however, be acknowledged, whereby the infiltration and disruption of critical systems, equipment and services could directly influence the lives of patients and vulnerable members of the community, and cascade out to affect health provisions across society more broadly. This could be accomplished with tools purchased through crime-as-a-service offerings that can facilitate ransomware attacks, as noted earlier in the report.

Preparedness to respond to cyber-attacks needs to be proportionate to the risk, scale and types of services being delivered

This applies in different ways to other essential services, including emergency services and transport networks, for example. A ransomware campaign targeting the Toronto Transit Commission's ICT network in October 2021 caused the internal email system to shut down. Online bookings were unavailable and the system used to communicate with vehicle operators was lost.[95] Vehicle operators switched to radio to communicate with Transit Control and travellers were urged to make reservations by phone.

The response avoided significant service disruptions and underscored the importance of redundancy planning and reliable communication links. Nonetheless, the incident resulted in the probable loss of the personal information of 25,000 current and former employees.[156] In the absence of resilient response measures, such an attack might confront a transport network with severe logistical and operational challenges. It follows that preparedness to respond to cyber-attacks needs to be proportionate to the risk, scale and types of services being delivered.

An attack on or within cyber-based infrastructure can have significant cascading effects. Consider how transport (aviation, maritime and waterborne, rail and road), power stations (electric and nuclear), water and sewage treatment plants, lift and escalator systems, traffic lights, long-distance pipeline systems and much more are largely automated. As we move to driverless cars, trucks, buses and smart homes or fully automated buildings with heating, ventilation, air conditioning, lighting and plumbing systems, the attack surface will increase. As critical infrastructure becomes increasingly digital and interconnected, the need to ensure it is protected and future-proofed becomes more urgent.

The US Cybersecurity and Infrastructure Security Agency lists 16 sectors whose "assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof".[97] The list includes healthcare, energy and water, emergency services and communications.

Communications – specifically satellite communications – are reflected in a high-level research paper by Chatham House, which noted how "critical infrastructure… depends on the space infrastructure, including satellites, ground stations and data links at national, regional and international levels".[98] It goes on to note the "requirement for increased protection against an increasing number of sophisticated and well-resourced cyber-related threats from nation states, terrorist groups, organised criminal groups and individuals aiming to steal intellectual property, cash or sensitive personal data, or simply to cause damage".[99] "Orbital infrastructure has become essential to communication, geospatial positioning, environmental monitoring, data linkages and defence, which raises concerns about its vulnerability to threats such as cyber-attacks".[100]

Landing back at a city level, a DDoS attack on a telecommunications company could cascade out and affect emergency services, and interference with the communication channels of a transport network could cause gridlock and widespread disruption.[101] In a low-probability, high-impact scenario, operational disruptions of a power plant could cascade out and impact on hospitals, residential areas, sanitation and water services. A cyber-attack, whether cyber-enabled terrorism or conducted by a cyber-criminal, could trigger unintended and/or unpredictable second- and third-order cascading effects.[102]

Further analysis of vulnerabilities at a city level, mapped against the implications and ripple effects of a successful attack, would be prudent to inform necessary developments in security. *'The Protection of Critical Infrastructure Against Terrorist Attacks: Compendium of Good Practices'*, produced by the UN and Interpol,[103] acknowledges the potential threat posed by cyber-attacks on critical infrastructure and is likely to be updated to address this more specifically.[104]

Several important lessons can be drawn from the cases discussed above: a) ICT systems, even if segregated, each on their own can affect overall business continuity; b) keeping critical infrastructure running is probably the most essential task to prevent second- and third-order effects; and c) exercising a variety of different system outages and having emergency plans in place to deal with cyber-attacks anywhere within a city's ecosystem must be a priority for city administrations and their constituent authorities.

Essential services

From a systemic point of view, cities are massive information ecosystems that collect, host and transmit data for a variety of purposes. Anything from schools, hospitals and police departments to public transport networks and administrative systems have to function reliably to maintain a sense of public order and normality in everyday life. The ICT networks of any of these organisations function as their own separate ecosystem, although they will probably share similar hard- and software, and are at least to a degree connected with those of other key actors in the same sector.

Thus, the networks in one hospital are far more similar to the network in another hospital than they are to the networks within a supermarket or the emergency dispatch service. Usually, these individual ecosystems are not substantially interconnected.

This means that although hospitals should network to some extent with other hospitals, an adversary that breaches a city's central systems should not be able to pivot from there into the servers of a police department. However, the widespread use of enterprise solutions by many sectors creates the possibility of common vulnerabilities, as shown by publicly known instances of such network overlaps. These demonstrate the far-reaching implications of security shortcuts.

> **Hostile actors including terrorists can use data theft and the aggregation of data, for example, to research, plan and support real-life (physical) attacks. Even small data thefts can be performed over a long period to slowly map a potential target.**

Experience-based accounts prove the importance of preventative planning in making network architectures more resilient and hardening the overall security posture. In a case resonating with the threat perspectives of city-level authorities around the world, a US police department was hit by a ransomware attack that began with the printers in the department not working. The incident was solved by restoring the system from 10-month-old backups and no ransom was paid. When malicious actors regained access, however, it was found that the department's security vendor provided administrator access for the entire network to many people – including the Mayor, his secretary and the entire city council.

Testimony from the US Secret Service highlighted the trade-offs between user convenience and security made in developing this architecture. This configuration left the gatekeeping parts of the internal network exposed to the internet to allow people to log in remotely. It also made it possible for these users to log in with administrator rights, granting them "full permission to change anything they want or do whatever they want in the network".[105] The consequence of this was, after an initial phishing email to the Mayor, that the attacker could watch how the Mayor accessed the police department's server to check his email. The attacker tracked all the log-in details and with these credentials was able to infect the police station with ransomware and launch a second attempt after an initial recovery.

To address these concerns, the city had to take disruptive remedial steps, including changing the security vendor and completely redesigning the network from the bottom up. The police department wiped all of its computers, including those in its patrol cars, changed and updated all passwords, reinstalled virtual private networks and became "more vigilant about restricting the permissions that were given to staff", based on the need for access.[106] During the remediation efforts, the Attorney General revoked the police department's access to certain resources as a precaution, including the system that law enforcement officers use to check a suspect's identification, such as when checking a licence plate during a traffic stop.

The loss of access to information and the exfiltration of sensitive police data are two of the main impacts to consider here. Hostile actors including terrorists can use data theft and the aggregation of data, for example, to research, plan and support real-life (physical) attacks.

Even small data thefts can be performed over a long period to slowly map a potential target. Reflecting on the case above, it is unlikely but feasible that a sophisticated adversary could create the opportunity to erase electronic evidence in a pending case, falsify police records and personal files, or maybe even issue an arrest warrant for a random person. In such a position, an adversary could also run campaigns against other targets by inserting malicious messaging into existing email conversations of the police department and the Mayor's office.

Such accounts underscore the importance of security practices that help ensure the resilient operation of essential services.

Central to this is the segregation of networks with a clear understanding of the infrastructure set-up and interfacing systems, as well as strict management of access permissions, combined with visibility of who is doing what on the network. The persistence and sophistication of attack and/or failure to adhere to strict security practices can lead to devastating outcomes.

In another case highlighting the risks related to the exfiltration of sensitive police data, a hacker accessed "10 years of data from over 200 police departments, fusion centres and other law enforcement training and support resources". This trove of data was released to the public in mid-2020, calling attention to the specific risks that political hacktivism may pose.[107] In the aftermath of the riots and protests in many US cities over the killing of George Floyd, DDoSecrets published this 270GB dataset known as "BlueLeaks" in June 2020.[108]

The persistence and sophistication of attack and/or failure to adhere to strict security practices can lead to devastating outcomes.

The records emanated from "the largest published hack of American law enforcement agencies… it provides the closest inside look at the state, local and federal agencies tasked with protecting the public, including government response to Covid and the BLM protests".[108]

Although DDoSecrets deleted close to 50GB and scrubbed some sensitive data related to crime victims, children, healthcare and retired veterans' associations, it is likely that sensitive data was missed.[109]

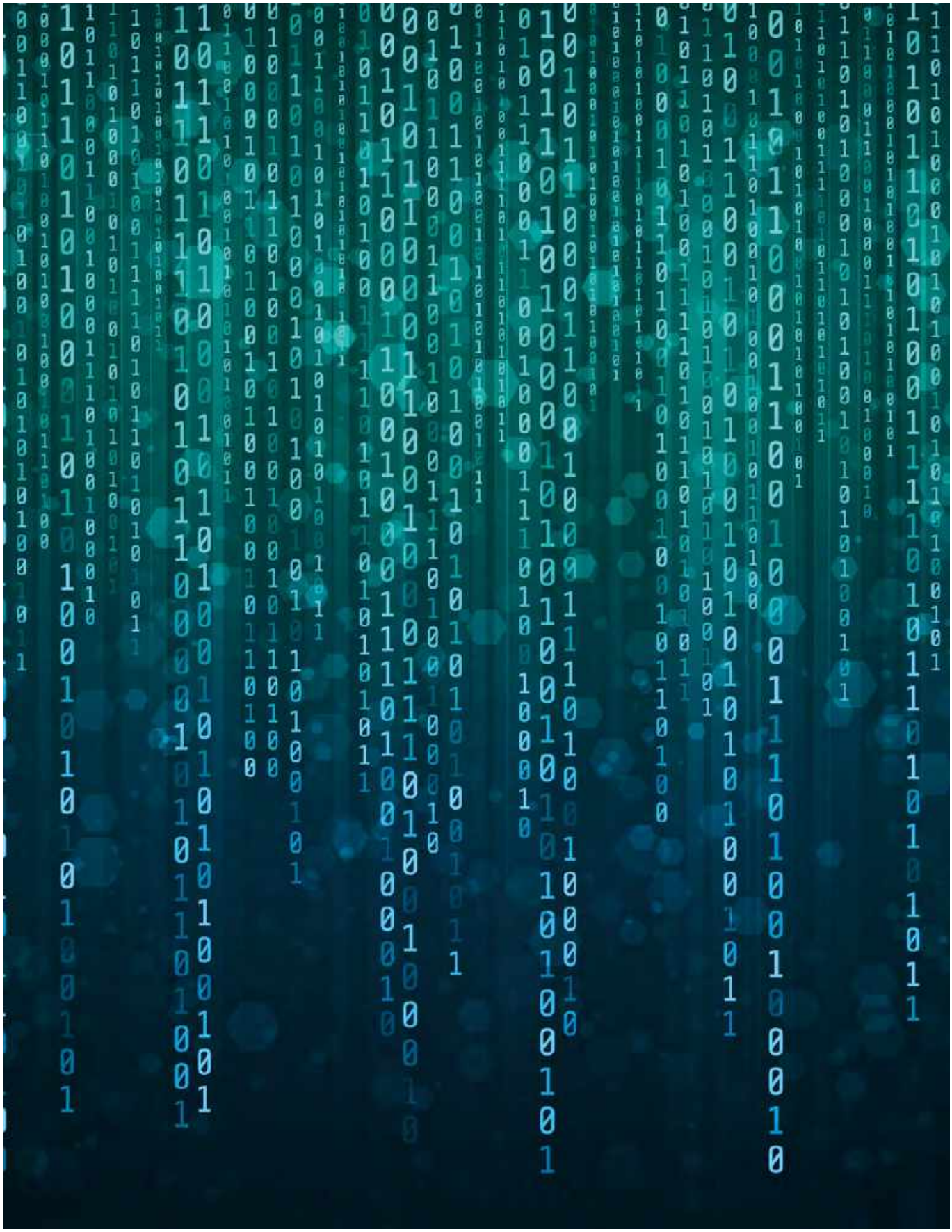
Included in the millions of files is the personal information of more than 700,000 US law enforcement officers, password histories, invoices, names of informants, detailed incident maps, videos and audio files, training materials and much more.

A former Assistant Secretary of Policy at the US Department of Homeland Security and General Counsel of the National Security Agency explained that "with this volume of material, there are bound to be compromises of sensitive operations and maybe even human sources or undercover police", putting lives at risk.

He noted that "every organised crime operation in the country will likely have searched for their own names before law enforcement knows what's in the files, so the damage could be done quickly".[110]

Although it is still unknown how exactly the BlueLeaks files were taken, two aspects are noteworthy: a) according to the National Fusion Center Association, "Preliminary analysis of the data contained in this leak suggests that Netsential, a web services company used by multiple fusion centres, law enforcement and other government agencies across the US, was the source of the compromise";[111] and b) investigative efforts to recreate the breach out of several artefacts in the leaked files revealed the use of a common hacking technique to gain widespread access to databases and the extraction of files.[112]

Upon publication of this report, BlueLeaks remains publicly available. In a further example, Aum Shinrikyo was found to have software that tracked 150 police vehicles in March 2000. It is an open question whether this form of anti-government hacktivism can be characterised as a distinct form of cyber-enabled terrorism, since it could be used to target specific law enforcement officers and members of the public.



Two notable findings are: a) events in real space can lead to targeted campaigns in cyberspace. This can include anything from website defacements and persistent DDoS attacks to the leaking of sensitive data and destructive campaigns; and b) a simple vulnerability in a single, widely used product can cause significant consequences at scale, as also evidenced by Log4j.

A logging tool known as Log4j – which is embedded in millions of commercial and open-source programs for web servers, email headers, usernames on social media and many other applications – was compromised.[113]

In December 2021, malicious actors began to actively exploit the vulnerability by syphoning data, stealing system credentials and installing tools to surreptitiously generate cryptocurrency tokens onto vulnerable systems. Meanwhile, organisations rushed to work out where and which of their applications were using the compromised tool, and whether their systems had been penetrated.[114]

Many organisations are likely to remain vulnerable to such deep-seated security flaws for prolonged periods, given the layered complexity of identifying systems at risk. This, as has been discussed, presents serious consequences for essential services and city administrations, and by extension the societies they serve.

Data exfiltration and destruction

The exfiltration of data for an adversarial campaign has become more and more common as ransomware groups use data leaks or the threat of leaking sensitive data to the public to increase the pressure and likelihood of a ransom payout, for example. In contrast to such financial and reputation-driven operations, some groups have specialised in destructive campaigns for political purposes.

Moses Staff is a hacking group that exclusively targets Israeli organisations by encrypting systems and leaking the victim's data without entering into any kind of ransom negotiations.[115] Its self-professed political goal is to "fight against the resistance and expose the crimes of the Zionists in the occupied territories".[116] According to Israeli security company Check Point, Moses Staff gains initial access to victim networks by presumably: a) exploiting known vulnerabilities in publicly facing infrastructure or exchange servers; b) moving laterally with basic tools for remote command execution; and then c) using open-source tools to perform volume encryption and lock the victims' computers.[117]

When compared with notorious ransomware crime groups such as Conti or REvil, Moses Staff's modus operandi is fairly simple. However, given that the group is driven by purely political motives, what matters in the end is not the technical sophistication of its operations but the knock-on effects its campaigns create.

Its attack pattern includes high-frequency operations against a wide array of Israeli companies and government entities with resonating effects through sheer quantity;[118] skilfully produced propaganda videos to show the exfiltrated data to the world – including a detailed 22-terabyte 3D map of Israel that was probably produced by the Israeli Ministry of Defence, thus taunting and embarrassing the Israeli defence establishment and exposing potentially sensitive data;[119] and even releasing the records and pictures of members of the Israeli Defense Forces, thus exposing personally identifiable information.

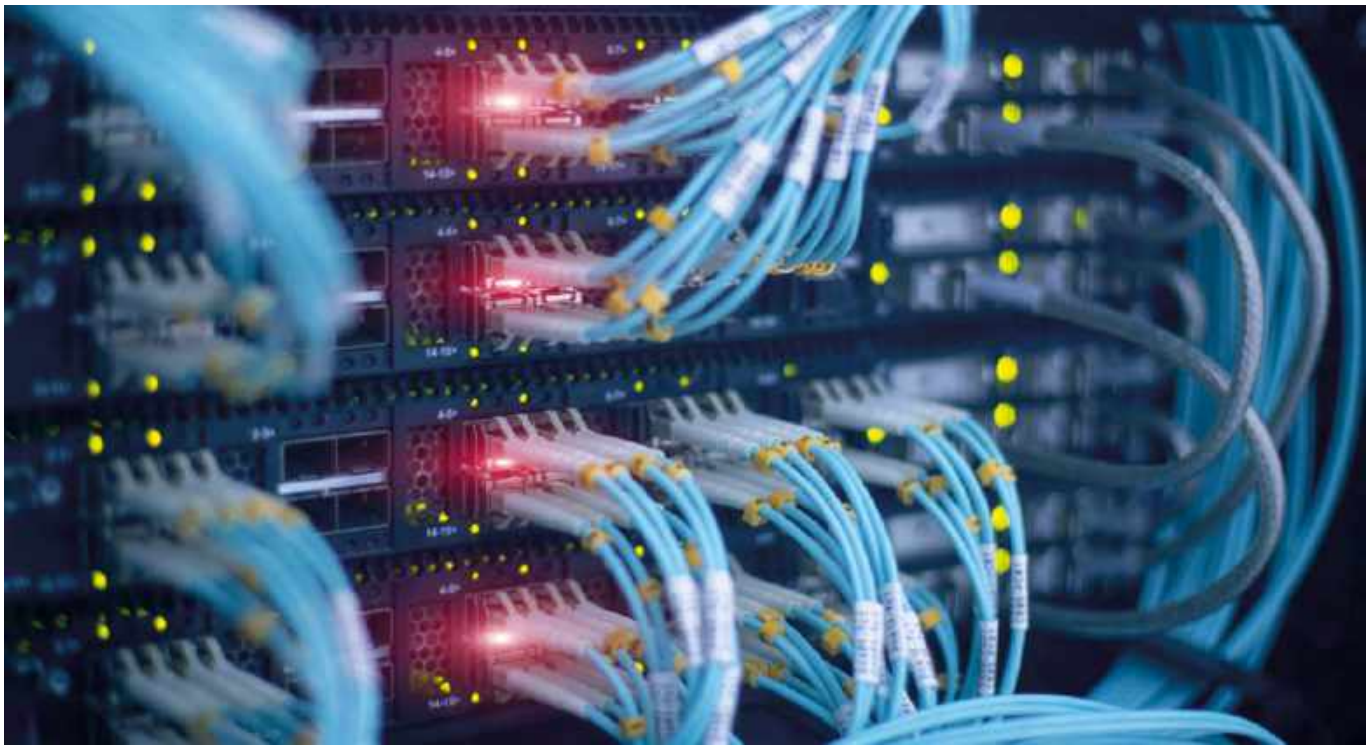
The enduring existence and continuous success of Moses Staff may form a blueprint for other politically motivated groups to emulate this behaviour outside the Middle East. In a scenario of global applicability, actors could try to copy the approach of Moses Staff and combine it with effects similar to the Colonial Pipeline attack in order to disrupt supply chains and the functioning of essential services.[120]

Similarly, an extremist group could target a variety of government systems in and through cyberspace with destructive campaigns, such as the targeting of the Iranian railway system by the anti-Iranian government group Indra in July 2021.[121]

Two dynamics that point to the potential for harm and abuse by a wide set of actors are central to these observations: a) destructive attacks do not have to be sophisticated to cause irreparable damage; and b) knowledge transfer and tactical adaptation is an everyday occurrence in cyberspace. Cyber-criminals learn from nation states, nation states learn from hacktivists and hacktivists learn from cyber-criminals.

Many organisations are likely to remain vulnerable to such deep-seated security flaws for prolonged periods, given the layered complexity of identifying systems at risk. This, as has been discussed, presents serious consequences for essential services and city administrations, and by extension the societies they serve.

In January 2021, a security researcher disclosed two vulnerabilities in Microsoft Exchange Servers – collectively known as ProxyLogon – that, if chained together, made it possible to remotely run any code on a targeted system without needing proper authentication.[122] An advanced persistent threat (APT) actor was found to be leveraging this in their campaigns. In March 2021, the company released two urgent patches to fix this first set of vulnerabilities.[123]



Further research revealed six more vulnerabilities in Microsoft exchange servers that needed to be patched. Chained together, these are now known as ProxyOracle (an attack that can recover any password in plaintext format) and ProxyShell,[124] which have been actively exploited by ransomware groups.[125]

The challenge that remained was how to quickly patch the hundreds of thousands of exchange servers worldwide that are vulnerable to these security flaws. Indeed, patching the vulnerabilities does not guarantee that a server is secure, as adversaries might have compromised a system and set up remote-access interfaces to achieve a foothold before the patches were installed. In a rather unusual step, a judge granted the FBI a warrant in April 2021 to remove any such entry points that the Bureau detected and had access to.[126]

Although it is not known how many times the FBI successfully intervened, a Slovakian cyber-security company reported that at least 10 other APT groups were taking advantage of the back doors that had been created.[127]

Particularly concerning attempts that sought to encrypt the data of targeted organisations without need for additional malware further highlight the importance of detecting initial intrusions to prevent harm. Tens of thousands of exchange servers worldwide remain vulnerable and have been exploited by ransomware groups and other malware operators.[128,129]

These other malware operators include criminal gangs infiltrating business emails as a means to distribute ransomware through trusted email accounts.[130] As one security researcher described it, "You've… got criminal gangs smashing and grabbing business emails now, then reusing them to spread ransomware access [and business email compromise campaigns] via legit email servers".[131]

Crucially, Luxembourg's Computer Incident Response Center noted that, when "the infrastructure is compromised… there is only one single procedure to ensure that you completely fix and mitigate the situation, close all potential back doors and kick out the attackers: reinstall every compromised server from scratch and then recover and copy the data over".[132]

However, effects are likely to be long-lasting. A "mail server is a highly valuable asset that holds the most confidential secrets and corporate data. In other words, controlling a mail server means controlling the lifeline of a company".[133] This highlighted the far-reaching implications of vulnerabilities in widely used software and proved how the preparedness and lifecycle management of software is key. This applies to other information including, for example, that held by laboratories, which could be particularly sensitive and detrimental, as the following case study indicates.

CASE STUDY
Laboratory ransomware attack

On 28 December 2020 a cyber-attack took place that targeted the General Medical Laboratory (abbreviated to AML in Flemish), an Antwerp-based laboratory analysing Covid-19 test results.[134] Early on, it was clear that this was part of a ransomware attack, aimed at obtaining a fraudulent financial benefit.

The AML, a private enterprise, handled about 3,000 Covid-19 tests a day, or about 5% of the national total in December 2020. As such, it was one of the largest private laboratories in the country dealing with the Covid-19 crisis.[135] Laboratory websites were bought to a standstill, together with some physical computers. A large part of the laboratories files, containing patient data of around one million people, was frozen. Extracting files in return for a ransom is a modern form of extortion but no data was stolen in this case.

Ten days before the ransomware attack, the laboratory had been the victim of another cyber-attack, in which malware was found on the servers.[136]

From that point onwards there was concern about further attacks and the possible accessing of sensitive data regarding Covid-19. Therefore, as soon as the AML experienced the second attack, it disconnected the network hosting its websites.

A few weeks later it became clear that several laboratories (also those in Genk, Moeskroen, Brugge en Ardooie) had become victims of the same ransomware attack and had suffered similar consequences.[137]

Studies show that once companies are attacked by ransomware, their mentality changes abruptly. Most companies invest in preventing new attacks. Strangely enough, this can lead to even more incidents.[138] This is probably due to the higher alert level on possible threats and the effective use of anti-cyber-attack systems.

Companies and governments are hiring more ICT specialists, hoping that this will prove useful when under attack again or when cleaning up the aftermath. Installing better systems is closely connected to enhancing cyber-security and investing more in the prevention of cyber-attacks.[139]

The current legislative framework also needs to evolve. In the US, the Biden administration is allowing emergency legislation in cases of large cyber-attacks. By contrast, in Europe most investigations tackling cyber-attacks are struggling with the GDPR legislation, when in fact then there is an urgent need to share certain information (for example, IP addresses and involved domains) quickly.[140]

Case study courtesy of Antwerp Police Department, as provided by Chief Inspector Roy Boes, Intelligence Division. The initial findings were made by the Antwerp police and further investigations were conducted by the Federal Computer Crime Unit (FCCU).

Psychological impacts

Persistent probing for vulnerabilities and continuous targeting by threat actors may develop a psychological facet that warrants closer attention, particularly in the context of cyber-enabled terrorism. Addressing ICT vulnerabilities can subject staff to high levels of stress over an extended period. In this way, adversarial tactics might – by design or coincidence – affect the psychological health of staff and others.[141]

Notably, a psychological effect has been at play during the ransomware campaigns during the Covid-19 pandemic, hitting everything from hospitals and schools to city administrations and private companies. The combination of stress, helplessness and urgency to get systems back up again probably contributed to many victims' willingness not only to pay the ransom but to do so more quickly than under non-pandemic conditions.[142] To date, little academic research has been done into these persistent and resonating psychological effects that can manifest themselves before, during and after a major cyber-attack has hit its target.

However, it could itself be a tactic to make cyber-attacks more successful (for example, through fatigue and stress on those protecting the networks). Cyber-security professionals, as a result of cyber-based work, have reported experiencing psychological effects like post-traumatic stress disorder (PTSD).

A first set of psychological studies and anecdotal accounts of cyber-crime victims offer a perspective into the nature of these implications. Analysis by the Centre for Counter Fraud Studies indicates that some cyber-crime victims feel violated, as if the attack was physical, and report psychological impacts such as anger, anxiety, fear, isolation and embarrassment.[143] These emotions can lead to a long-term breakdown in fundamental trust relationships, a general fear of technology itself or in extreme circumstances even suicide.[144] Research at the Cambridge Cybercrime Centre suggests that "depending on who the attackers and the victims are, the psychological effects… may even rival those of traditional terrorism".[145]

Cyber-security professionals who may have struggled to keep their company's network and data secure are likely to experience psychological effects. Such effects appear conceivable for IT staff at online-dating site Ashley Madison in 2015 and the Finnish therapy start-up Vastaamo in 2020, whose network breaches leaked highly sensitive personal information that destroyed many families, led to suicides and derailed the lives of countless others.[146]

Related to this direct psychological impact are other prevalent healthcare concerns in the cyber-security community that often lead to burnout and job fatigue. Contributing conditions include the enduring cyber-security skill shortage (understaffing and high turnover); long working hours (overworked staff and high workforce attrition); demand for persistent vigilance (causing high stress levels); and an ever-growing cyber-threat landscape that results in alert fatigue.[147]

Alert fatigue is probably the most interesting phenomenon in this context because it can manifest itself in longer security response times and missed indicators of network compromise – with devastating consequences. Alert fatigue is somewhat poorly defined in the academic literature, but it is generally accepted that it is a combination of desensitisation and cognitive overload because of the complexity and quantity of incoming alerts; reacting to actionable alerts and wasting time on chasing down false leads; and the constant fear of missing an incident.[148,149,150] The evidence relating to alert fatigue sends a strong signal to companies and governments to take care of cyber-security staff from the perspectives of mental health and security.[151]

Analysis by the Centre for Counter Fraud Studies indicates that some cyber-crime victims feel violated, as if the attack was physical, and report psychological impacts such as anger, anxiety, fear, isolation and embarrassment.[143]

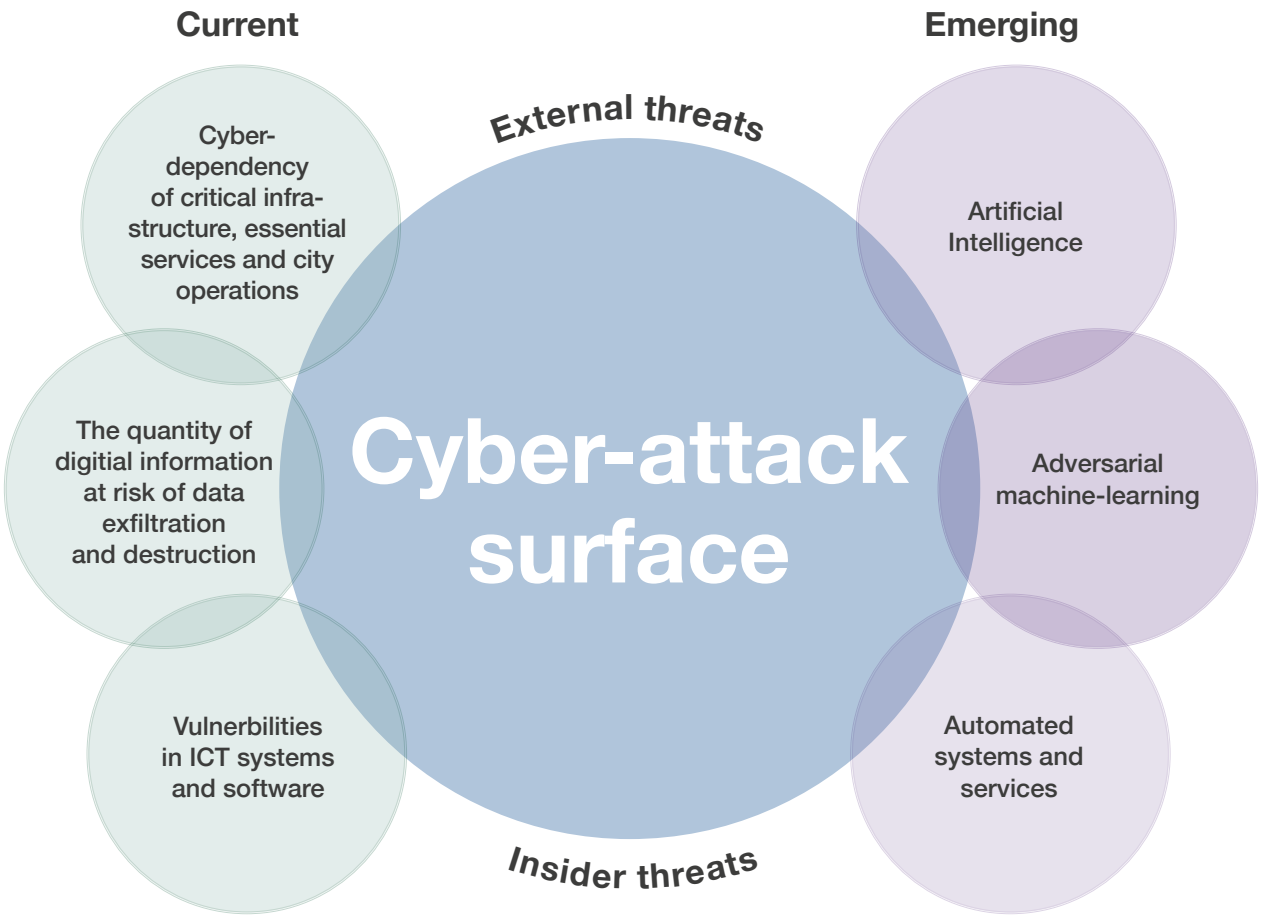
A system view of vulnerabilities

The psychological impact of cyber-attacks is a key consideration for city authorities, as are data exfiltration and destruction, impacts upon essential services and critical infrastructure, as explored above. This has pinpointed a set of system vulnerabilities that can inform and drive considerations for preparedness.

Notably, a simple vulnerability in a single, widely used ICT product can cause widespread significant consequences; destructive cyber-attacks do not have to be sophisticated to cause irreparable damage; and resonating second- and third-order effects may cause more collateral damage than the actual cyber-attack or incident itself. These cascading effects have the potential to significantly disrupt city operations.

As has been mentioned, cyberspace and ICT systems are used to operate and monitor critical infrastructure, essential services and city operations including the supply of commodities, goods and services. The "connectivity" race – societies' drive towards integrated technology – has exposed vulnerabilities. Findings to date have spotlighted the trade-offs (think sacrifices) between cost and convenience versus security as central to these efforts[152] and highlighted the importance of risk management. This risk-management process must relate to current cyber-threats and those that are otherwise emerging.

Vulnerabilities and emerging threats



3 Emerging Threats and Technologies

> **“Cyberspace provides a new delivery mechanism that can increase the speed, diffusion, and power of an attack, and ensure anonymity and undetectability.”**
>
> European Commission
> *‘The Landscape of Hybrid Threats: A Conceptual Model’*

As the preceding section has shown, the exponential integration of ICTs, especially IoT devices, into almost all sectors of economic and social activity, coupled with varying levels of cyber-security, have produced an expanded cyber-attack surface. This means cities are arguably becoming easier targets because their connectedness brings them within reach of actors that operate from a physical distance.[153] Even at a high level, the networked nature of city infrastructure shows a wide plane of potential vulnerabilities.[154]

Over the last few years, cyber-threat actors have exploited commercially available tools for their operations. Hacking tools are widely and freely available for use by skilled penetration testers, state actors, organised criminals, hackers and terrorists. Some of these tools were created with good intentions but have been used for malicious intent. There are many types of malware (viruses, trojans, worms, ransomware and spyware), for example, that could be used to adversely affect victim systems by gaining remote access, spreading across many domains and maintaining a foothold in the target network.

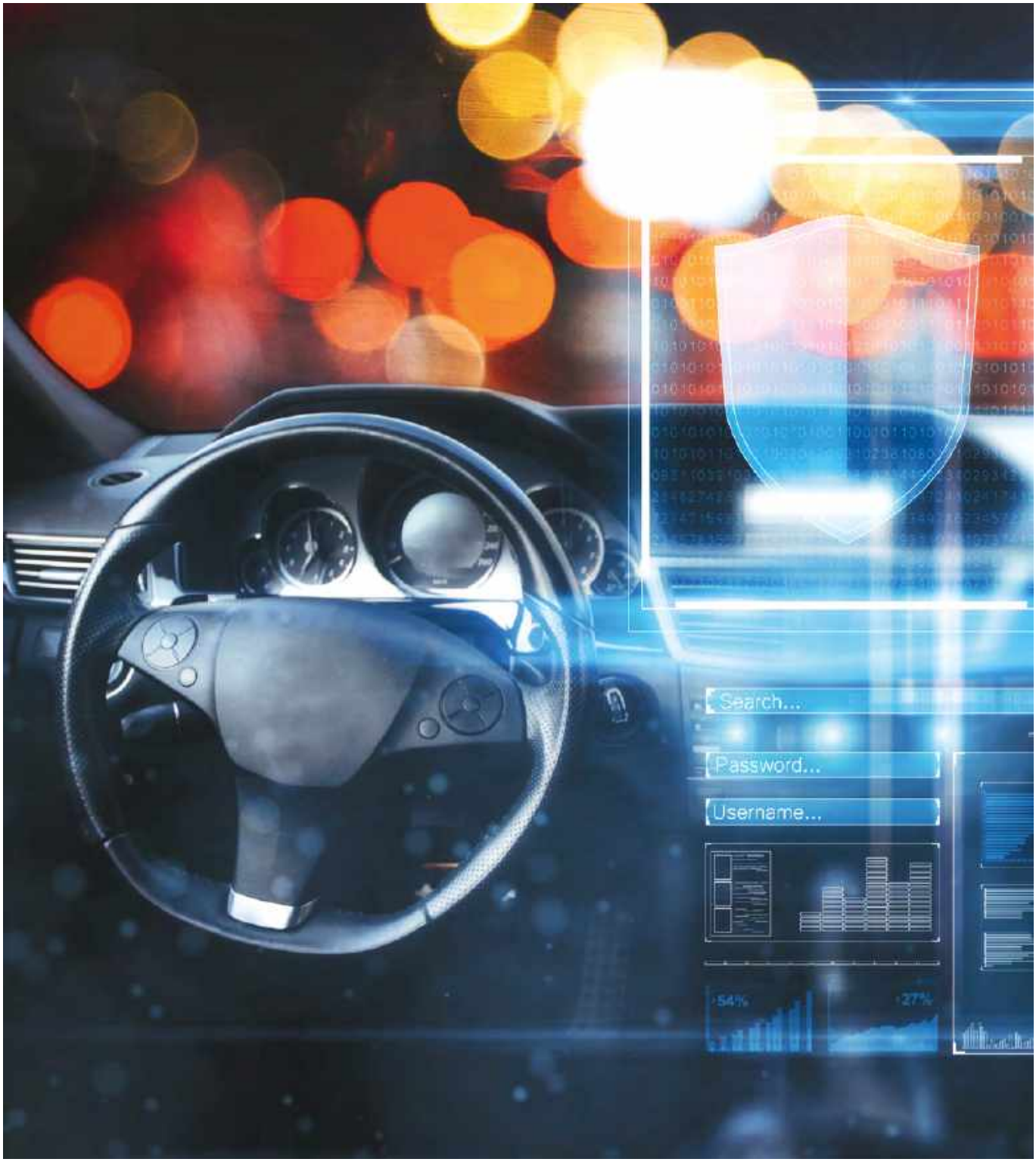
This horizon scanning, or consideration of the art of the possible, will call attention to the capabilities that might be of interest to terrorist groups and the impact they could have on critical infrastructure, essential services and city operations.

However, new threats are emerging, driven by rapid technological advances. This section will consider those technologies and methods that may exacerbate, or be exacerbated by, the cyber-threat. It will summarise what may be on the horizon, the potential exploitation risks and consequences, and how these could be exploited by hostile actors, including as cyber-enabled terrorism.

This horizon scanning, or consideration of the art of the possible, will call attention to the capabilities that might be of interest to terrorist groups and the impact they could have on critical infrastructure, essential services and city operations. This approach seeks to identify areas that need to be prioritised in terms of security and enables the consideration of scenarios to further inform planning and preparedness.

Artificial Intelligence in cyberspace

AI (the development of computer systems that can perform tasks normally requiring human intelligence) technology is being pioneered by nation states – some more than others. AI autonomous systems are widely being developed, or have already been implemented on the ground, sea or air. Israel’s Iron Dome missile defence system, for example, has an AI function that is trained to detect incoming rounds that might threaten civilian populations or military facilities.


Search...
Password...
Username...
54%
27%

Indeed, AI collaborations between states such as China and Russia reside in lowering the unit cost of mutually beneficial technologies. However, the fallout of this is that the cost of AI technologies is driven down and can be exported or acquired more broadly by non-state actors or sold via black markets. This diffusion of technology has the potential to happen quickly, giving non-state actors asymmetric advantages over states.[155] This will ultimately filter out to regions, cities and local areas.

The fact that cyberspace and emerging technologies transcend borders, are difficult to govern and regulate, and are entwined with society at all levels compounds the issue. AI, therefore, risks becoming another tool for cyber-enabled terrorism that can be used to automate specific tasks such as weaponising and programming commercially available drones to target individuals, ethnic groups or specific locations/infrastructure.

Although this would be a relatively sophisticated mode of attack, the fact that ISIS have been using drones in Iraq since 2017[156] puts this into perspective. Experience suggests that over time barriers to entry will erode (much as technologies that allow for drones and 3D-printed weapons are more accessible and affordable today than they were) and the capabilities of hostile actors in cyberspace will increase.

Just a few years ago, only highly resourced states and state-sponsored groups could develop and deploy cyber-attacks, online information operations and AI-enhanced technology. However, hostile actors including terrorists can now increasingly adopt these because of low-cost commercial availability,[157] generational shifts in related knowledge and expertise and a lack of regulation.

AI can also be used to maximise the impact of cyber-attacks by leveraging the machine-learning of large datasets to prey on vulnerable individuals financially or psychologically. Machine-learning offers a way to gain access to protected databases that contain sensitive information such as patients' health records and details of medical procedures.

Experience suggests that over time barriers to entry will erode (much as technologies that allow for drones and 3D-printed weapons are more accessible and affordable today than they were) and the capabilities of hostile actors in cyberspace will increase.

These techniques could allow for intentional leak or blackmail, or further compromise health where medical advances may include internet-based devices that can be manipulated. Machine-learning is considered in more detail later in this report.

The use of AI in cyberspace, however, is notable. It enables hostile actors to trawl the internet to identify online vulnerabilities; attempt to extort financial resources from companies or individuals; and generate disinformation at scale to manipulate a population group's views for political advantage.[158] Quantum computing takes this further, highlighting another avenue for a sophisticated cyber-attack. The power of quantum computing means that it can "crack the code" of encryption algorithms, leaving secure communication that is conducted across insecure internet networks vulnerable.

Cyber-attacks using quantum computing would probably focus on information stored and transmitted across public websites, email exchanges and common banking transactions.[159] In other words, any state or non-state actor that achieves quantum supremacy first could take advantage of inadequate digital security and make current encryption formats obsolete. Russia and China already have state-sponsored research programmes in quantum computing, aiming to gain superiority in offensive cyber-operations. China plans to invest $11 billion for a national quantum laboratory and the Russian Quantum Center reported in 2017 that its newly developed quantum computer could perform general computations.[160,161]

Current encryption formats urgently need to be revised to protect against quantum computer cyber-attacks, a process that could take at least a decade to implement.

The timeline for quantum technology becoming a viable cyber-security threat is uncertain, but immediate preparation is necessary when one considers that current encryption standards took two decades to establish.

Quantum technology poses unique changes for multiple facets of computer systems including soft- and hardware.[162] If effective cyber-attacks hinge on identifying and exploiting ICT vulnerabilities, it follows that the use of AI to scan for weaknesses in computers, networks and communications within a system would be beneficial to hostile actors and cyber-enabled terrorism. AI applications can identify outdated, unpatched or misconfigured aspects of ICT systems as markers of vulnerability.

These markers can make cyber-attacks cheaper, more accurate, targeted, convincing and automated – including the automated execution of cyber-attacks themselves.[163] Although terrorists are currently considered to be low-capability actors, it is proposed that it is a matter of when, not if, terrorists will seek to harness AI-enhanced cyber-applications and technologies.

This includes those that have the potential to inflict real-world consequences for critical infra-structure, essential services and city operations.[164]

Adversarial machine-learning

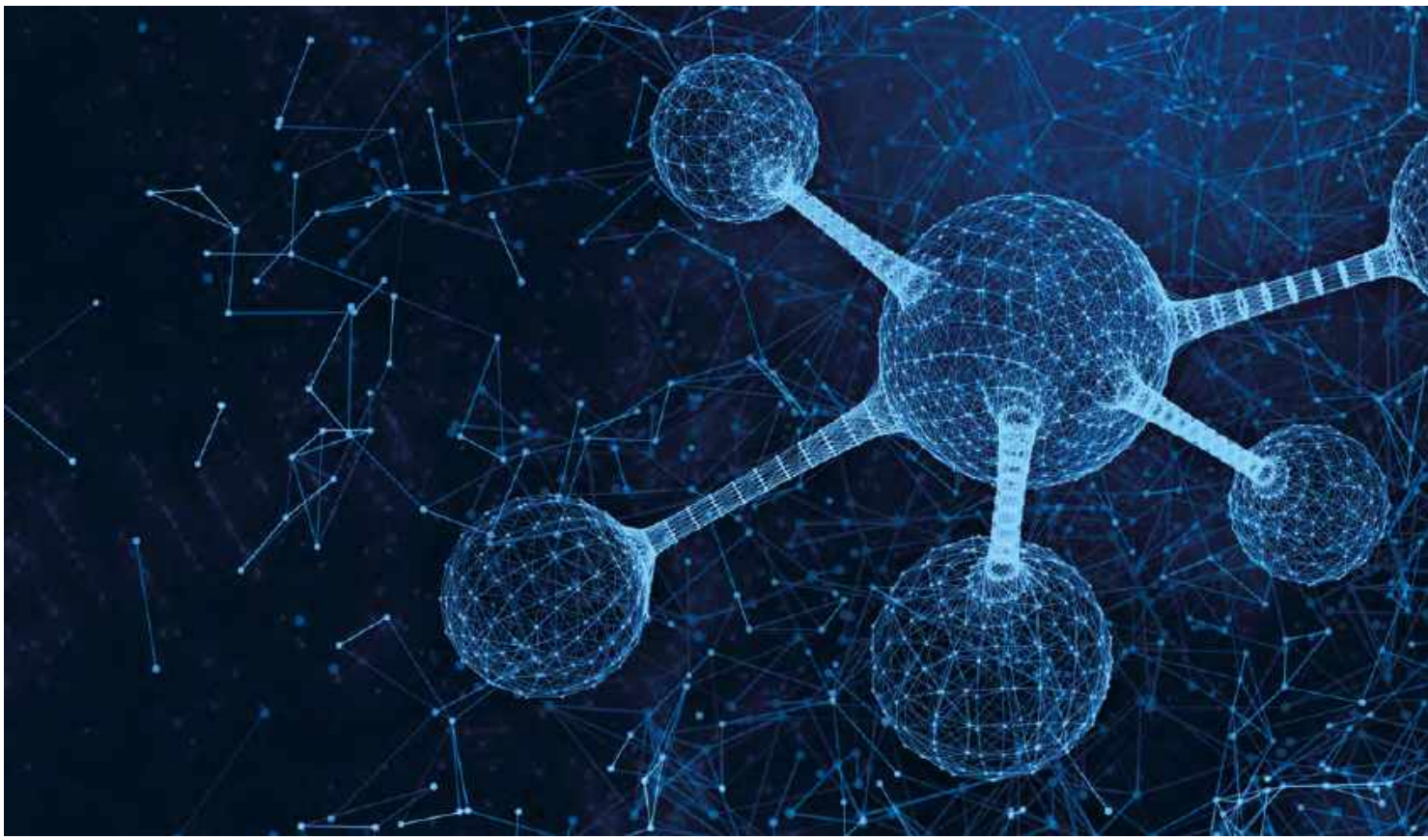
As cities turn to smart technologies, increasingly automated services such as public transport and utilities will rely on machine-learning to find areas for greater efficiency and better customer service. New-generation smart technologies depend on programming that incorporates AI into operating systems to achieve these benefits and provide data to city managers on areas for improvement. This can be understood as machine-learning – an AI technique that can be used in many fields, including cyber-security.

Responsible data scientists and developers build, train and deploy machine-learning models to recognise, defend and control data processes that build trusted results. However, the production of machine-learning systems is inherently vulnerable to "adversarial machine-learning". This is where hostile actors have the potential to attack these systems, manipulating them and changing their behaviour to serve malicious means.

One of the well-known applications of AI is autonomous vehicles. "Aside from facilitating attacks with fully autonomous vehicle-borne improvised explosive devices, it has also been suggested that self-driving cars could be used to cause serious accidents".[165,166] It would be feasible, albeit as a highly sophisticated form of cyber-enabled terrorism, for an actor to hack into and manipulate the coding of a self-driving car or smart bus and encourage the bus, for example, to recognise a pedestrian as a green light, or compute a pedestrianised area as a high-speed thoroughfare.

Although smart buses and other tools can be used to meet urban-planning initiatives, they can also be leveraged by adversaries who wish to undermine public safety.

If effective cyber-attacks hinge on identifying and exploiting ICT vulnerabilities, it follows that the use of AI to scan for weaknesses in computers, networks and communications within a system would be beneficial to hostile actors and cyber-enabled terrorism.



Another consideration is the potential to contaminate machine-learning systems to misclassify specific examples, causing precise actions to be taken or omitted. This might be by disguising antivirus software as malware and introducing it to critical infrastructure systems. By forcing the misclassification of antivirus software, an adversary could "trick" the system and leave it vulnerable and unprotected, thus exposing critical infrastructure to attack.

Furthermore, attackers with the right knowledge could also replicate a sophisticated algorithmic model, a financial-trading model for example, and use it to manipulate and hijack regular procedures and operations.

An example could be stealing a financial model to adversely affect proprietary algorithms intended for high-frequency stock trading in a specific market.[167]

Those behind the DarkSide ransomware group have announced that they are targeting companies listed on stock markets. This could cause significant disruption to the market and trading while providing a potential income stream for the perpetrators. DarkSide says it would also seek to enlist "insiders", or unethical stock traders.

Between 2018 and 2020, insider threats increased 47%, according to a survey of IT security experts in nearly 1,000 global businesses.[175]

Stolen proprietary algorithmic models could also be used for the purposes of espionage or reverse engineering, highlighting, in this case, the importance of proactively surveying the financial sector or others to identify and counter opportunities for malicious intent.

From a city perspective, financial hubs often form part of the city footprint but wield national and international economic influence, which creates an interesting dynamic in terms of preparedness and consequence management.

This applies to next-generation communication systems, where there is an increasing concern about how machine-learning could be used to spot vulnerabilities in 5G systems and tamper with the learning process embedded in 5G communications.

Due to the shared and open nature of the wireless medium, wireless applications are highly susceptible to adversaries such as jammers and eavesdroppers that can manipulate the processes of machine-learning over the air. Although there is increasing interest in this space, adversarial machine-learning has not yet been considered for sophisticated communication systems such as 5G.

This could change as interception equipment and techniques become easier to use and more readily available for threat actors, which could, in turn, cause grave degradation to communications infrastructure,[168] possibly resulting in massive service delays or failures, mass public panic and distrust.

The cyber-threat in specialist areas such as the biosciences should also be considered. Here, increasing dependence between digitalised platforms are coupled with emerging or converging technologies like the use of AI.

Not only could cyber-attacks expose information, formulas or genetic codes that could be manipulated for malicious means by terrorists and other hostile actors, but the use of AI to predict modifications to pathogens, for example, could be used to cause harm.[169,170,171,172,173]

There are robust security measures in place for these environments and such a cyber-attack, terrorism or otherwise, would be highly sophisticated and therefore unlikely, given current capabilities. Therefore, this is not a judgment on the threat or likelihood, rather an acknowledgement that the threats exist. It would only take one person with the access, knowledge and intent.

Prevalence of insider threat

According to the Director of the National Insider Threat Task Force, "foreign intelligence agencies are likely to ramp up their targeting of trusted insiders".[174] Although not considered a new threat vector, technological advances have made it easier for insiders to cause major damage to their employer knowingly or unknowingly. Between 2018 and 2020, insider threats increased 47%, according to a survey of IT security experts in nearly 1,000 global businesses.[175] This threat is amplified if hostile actors steal privileged users' credentials to gain access to a trove of proprietary information, such as supply-chain data or even national security secrets. From the perspective of a malicious insider, the goal would be either co-opting/recruiting the privileged user or being that user in the first place.

Likewise, the possibility of a hostile actor infiltrating ICT systems to gain physical access to premises should be acknowledged. Placing insiders in critical infrastructure could be used to destroy a system from within or to harvest details of targets.

Consider how an Al-Qaeda insider at British Airways now faces a life sentence for planning an attack, including the claim that he could access British Airways servers and erase all the data, causing massive disruption and financial loss. In evidence, witnesses said that the airline would lose £20 million a day if its IT systems collapsed.[176]

Indeed, the profile associated with the insider threat has evolved and continues to do so. Increased reliance and interconnectivity with internet-enabled components and the growing new world of remote working have further exposed computer networks and operating systems to the insider threat.

It is also worth noting how the insider threat could be generated by external factors, such as the targeting and extortion or blackmail of employees through the cyber-domain, for example, to effect a result.

Businesses and public sector entities that lack dedicated insider-threat teams are likely to miss internal threat indicators. Given the reported increase in insider threats, attention from organisations and city administrations is warranted.

Future-proofing technology

Emerging threats and technologies have been summarised in three key areas: artificial intelligence in cyberspace; adversarial machine-learning; and the prevalence of the insider threat. These reflect tangible, accelerating, threats that will continue to evolve. In five to 10 to 15 years' time, the landscape could be significantly different. Cyberspace, AI and machine-learning serve as enablers, just as "electricity powers a vehicle or the combustion engine accelerates a train" and is therefore useful to hostile actors.[177]

This has only scratched the surface and hasn't considered the regulation and control of commercial robotics, for example. Moreover, some national security experts even warn that terrorists will eventually use virtual-reality technology in their recruiting, training, rehearsal and logistical planning, and to conduct attacks in the real world. This concern becomes more plausible as virtual-reality technology becomes more popular, cheaper and realistic. The virtual-reality marketplace is rapidly expanding; companies such as Facebook, Google, Microsoft, OnePlus and HTC are competing in a global market that is projected to reach nearly $84 billion by 2028.[178,179]

> **Looking to the future, it is plausible that cyberspace, AI and machine-learning could be harnessed to attack just about any system built on technology.**

These newer technologies, including augmented-reality systems, may not have the same encryption standards as conventional platforms. Third-party components, along with loose regulations, may not sufficiently prioritise security (this is the same trade-off or sacrifice between functionality and security that has already been flagged in this report). These systems may increasingly process personal biometric data such as facial features, eye structure and speech patterns.

Systems storing unprotected sensitive biometric data are ripe targets likely to be exploited and will require extensive monitoring. Many scenarios can be imagined – information manipulation in this space, for example, could cause real-life consequences.

Certain cyber-trends related to augmented reality, like the game Pokémon Go played on portable electronic devices, also connects the virtual with the real world, thus causing effects. When the game was launched, people playing the game were widely reported to be crossing streets without looking and ending up in dangerous areas or causing traffic congestion.[180,181,182] This type of trend could be exploited to influence hundreds or thousands of people to move en masse, slowly or quickly, to a certain geographical point, thus straining public transport and blocking roads. Although perhaps unlikely to be used as a form of cyber-enabled terrorism, this is another example of a real-world event that may serve as inspiration.

Looking to the future, it is plausible that cyberspace, AI and machine-learning could be harnessed to attack just about any system built on technology. A recent UN paper flags an early warning for potential malicious uses and abuses of AI by terrorists.[183] Although not the focus of this report, the use of new technologies (such as weaponised drones with AI capabilities) to deliver physical attacks is also of concern. Further research on the malicious use of AI and machine-learning is urgently needed. Although the links with cyberspace are clear, they are complex subject matters in their own right and deserve further attention.

The emerging threats and technologies explored in this section remain under-regulated and under-governed. This is perhaps in part because effective or feasible policy responses are unlikely to consider outright bans on AI or AI-enhanced technology because of its diffuse nature and questions of enforceability. This dynamic, evolving and rapidly advancing environment also makes restrictions very difficult to implement. Instead, "public-private partnerships will be key in incorporating software restrictions".[184]

It follows that a higher degree of governance and private sector regulation would be prudent, perhaps conducted under the umbrella of an international agency mandated to provide oversight. A charter detailing ethical standards of use would support democratic societies in holding non-state actors to account when AI is misused. At a national level, the bolstering of defence measures and forensic capabilities needs to be coupled with a drive to enhance the domestic talent pool of science, technology, engineering and mathematical capabilities.[185]

These principles translate to cyberspace more broadly through the need to agree approaches for handling cyber-threats, holding hostile actors to account and investing in cyber-defence expertise and capabilities. This brings us back around to the cyber-threat itself.

As the preceding section outlined, cyberspace presents several notable vulnerabilities for cities related to critical infrastructure, essential services, data exfiltration and destruction and psychological impacts. This is coupled with a foresight-based perspective on emerging threats and technologies and the use of AI in cyber-attacks. The core challenge is how cities can prepare today to be ready for tomorrow.

4

Implications for City Preparedness

> **It's time for a new security model that addresses the full attack continuum – before, during and after an attack.**
>
> Gordon Feller
> *'Protecting Our Cities from Cyber-Attacks'*

Cities are complex urban environments – a geographical footprint with a mass of people, industry and infrastructure that intersect across inherently interdependent layers of structures, systems and services. They are often defined by their urban extent (the spread of built-up structures) and/or degree of urbanisation (the share of local population living within the city's boundaries).[186]

The composition of a city usually includes a relatively high proportion of industry and population density, national and local authorities, as well as high-profile sites (such as government facilities, critical infrastructure, tourism hotspots and famous venues).

Cities also wield significant political and economic influence and authorities are required to maintain and deliver vital societal functions.

Vital societal functions in a city present many cyber-attack vectors, including physical infrastructure and software services. This has been demonstrated within the preceding sections, as have the cascading effects that a cyber-attack could have upon the urban ecosystem, given the concentration and proximity of infrastructure in densely populated areas. Three core factors serve as vulnerability drivers and therefore influence the cyber-threat in cities:

1. **Convergence**
   The convergence of infrastructures that blur the divide between physical and online worlds enables cities to control and govern technological systems through remote cyber-operations, but this also exponentially expands the cyber-threat landscape.

2. **Interoperability**
   The coexistence and frequent interactions between old and new systems and platforms can create a disparate cyber-ecosystem with hidden security vulnerabilities.

3. **Integration**
   The integration and comingling of domains through the IoT and digital technologies mean that a problem in one service area could quickly cascade into other areas and potentially lead to widespread and catastrophic failures.[187]

It follows that cities can make for easy targets with multiple entry points, intensified by a city's size and organisational structure that will have grown organically long before cyber-security became an urgent matter. Preparing cities for future cyber-attacks may therefore involve the arduous task of patching one vulnerability, only to find another.[188] The digital revolution means cities are becoming increasingly automated, with a range of emerging and converging threats and technologies to match. It follows that a city's ability to respond to cyber-threats is dependent on its preparedness. In many respects, the preparedness and resilience of cities are the building blocks for the preparedness and resilience of nations.

Preparedness includes many factors, some specific to local circumstances, some broadly applicable to most cities. This section will focus on the latter, to emphasise that a cyber-attack on a city-wide scale, or with city-wide implications, will require multi-agency collaboration that is underpinned by a joint level of understanding, preparedness and resilience.

Cyber-security in cities

The term "cyber-security" needs a broad application in a city context. As mentioned before, it includes securing data communication and access to societal services, and critical infrastructure that could be affected by a cyber-attack, such as water and power supply or transport networks. Cities also need to consider the parameters of large-scale redundancies and continuity.

A city's ability to respond to cyber-threats is dependent on its preparedness. In many respects, the preparedness and resilience of cities are the building blocks for the preparedness and resilience of nations.

Information security, for example, is vital in a strategic sense and is, therefore, perhaps one of the most important measures for a city to strengthen in a cyber-security context. Consider the damage that could be caused by breaches that expose sensitive information such as high-risk sites, the locations of high-profile public figures or covert operatives, confidential correspondence, emergency service databases, as well as health and social care records as demonstrated earlier in the report.

Such exposures could be significant and detrimental, with implications for city authorities and possibly national security. The protection of information, data systems and software services is usually handled within each responsible organisation through dedicated ICT (information technology) experts; security measures (for example, firewalls, traffic filters, load balancing and re-routing, as well as virtual desktop infrastructures); the vetting and training of staff; and business-continuity arrangements.

Methods to assess risk and information control are also employed, such as the CIA ("confidentiality, integrity and availability") triad.[189]

This, coupled with "assumed breach/zero trust" as a method for risk acceptance and constantly adapting security measures to the current threat landscape can mitigate many obvious risks. However, a global survey of business leaders identified that nearly two-thirds expected the cyber-threat to increase.[189]

The key is to identify what needs to be protected, what it needs protection from, and in what way it needs protection. Traditionally, this responsibility sits within, and must be applied within, each organisation, which is difficult to pursue and oversee from a city perspective.

This also applies to the protection of cyber-based infrastructure, including systems that are interconnected, such as fibre-optic network grids, but also largely segregated systems, such as industrial controls for power plants. Typically, these types of critical infrastructure are operated by providers from national or local authorities or by private enterprises sourced from within an open market, where operations rely heavily on external resources.

The key is to identify what needs to be protected, what it needs protection from, and in what way it needs protection.

The provider owns the end-to-end service and is usually required to abide by national regulations to ensure that critical infrastructure maintains a certain quality of delivery, contributing to resilience and robustness.

These regulations typically include demands of redundancy, high physical security and a mandatory routine to report any interference or disruption.

It follows that cyber-security in cities is underpinned by the ability of individual organisations to block as well as detect and remediate cyber-attacks. Although there is a clear need for organisations to ensure that they continue to invest in ICT; future-proof security of information; protect infrastructure; and reinforce business-continuity arrangements, this is organisation-specific and there is already ample guidance available.[190,191,192]

This report, therefore, recognises organisations as the first line of defence against a cyber-attack but is concerned with those attacks that break these defences (either through inadequate security or advanced modes of attack) and manifest with real-world implications.

In other words, the report proposes that simple attacks that cause containable damage are likely to give way to modern cyber-attack operations that can be sophisticated, well funded and capable of causing major disruptions. Defences that rely exclusively on the detection and blocking of cyber-threats for protection are no longer adequate.

In his article, *'Protecting Our Cities from Cyber-Attacks'*, Gordon Feller stated, "It's time for a new security model that addresses the full attack continuum – before, during and after an attack".[193] In this context, building layers of resilience into cities at a regional level is key.

Prevention and protection

An obvious way to strengthen prevention and protection is by promoting a robust approach from the public and private sectors, cultivating and implementing a culture of deterrence and security and ensuring this is central to the security and development strategies of city administrations.

In this respect, cyber-governance is essential to set policy and regulation and provide a clear direction. At an international level, the EU Network and Information Security Directive[194] offers a legislative example, whereby every EU Member State has started to adopt national legislation, which then aligns with the directive.

The directive has three main parts: national capabilities, cross-border collaboration and national supervision of critical sectors. For a city, this requires active measures and management to fulfil obligations that increase resilience. This is, however, accompanied by the challenge of translating laws and policies at the local level as well as across localities.[195]

The EU Cybersecurity Strategy for the Digital Decade also "points to a significant investment in cybersecurity operations capability. However, implementation will inevitably be patchy and offer limited protection across supply chains".[196]

Cyber-security is akin to fire prevention; it needs a systematic approach as part of a long-term strategy… it means identifying and mitigating system vulnerabilities; strengthening protective security measures and continuity arrangements for city operations; enhancing the capacity and capability of agencies to respond to and recover from an attack.

Governance and policy at a city level is fundamental in reducing digital dependencies and the threat of cyber-attacks by securing financial allocation for infrastructure development, continuity planning and multi-agency preparedness. Embedding cyber-resilience as a political priority can strongly influence and contribute to multi-agency collaborations and progress.

It follows that a city-based authority or municipality may also consider the possibility of taking strategic ownership of cyber-based infrastructures to ensure by active governance independent access to network resources.

Cities could also better promote, stimulate or demand a high level of preparedness through private sector collaboration and careful outsourcing. This requires a coordinated approach between city authorities as part of a long-term action-orientated strategy with sustained investment and clear lines of accountability.

Furthermore, a city can offer targeted economic stimulation or other incentives for important small to medium organisations that sometimes lack the funds necessary to achieve a high degree of preparedness or resilience in a cyber context.

One example, from the City of Stockholm, is to build a local city-based fibre-optic network between critical points, thereby stimulating the local market for fibre-optic networks and thus affordability through competition.[197] Cities should also consider building redundant backbones for communication in case of loss of internet connection (the Swedish Netnod initiative[198] provides an example).

A platform of collaboration could also be created, whereby organisations commit to certain cyber-security measures in exchange for collaborative support in the event of an attack.

Cyber-security is akin to fire prevention; it needs a systematic approach as part of a long-term strategy. Prevention and protection, however, must go far beyond this. They require investment and buy-in at the highest levels of organisations, multi-agency collaboration and a holistic, forward-thinking approach.

It means identifying and mitigating system vulnerabilities; strengthening protective security measures and continuity arrangements for city operations; enhancing the capacity and capability of agencies to respond to and recover from an attack, while developing and integrating technology (using tested, certified and trusted components) into cities and infrastructure in an intelligent way.

The latter is captured, in part, by the smart cities agenda and associated strategies such as “Smarter London Together”, which outlines the city’s priorities and roadmap, including enhancing digital leadership and skills, and improving city-wide collaboration.[199]

London's City Resilience Strategy also recognises the need to develop capabilities to respond to the consequences of a cyber emergency[200], a need that will resonate with cities globally.

However, overall preparedness for accelerating cyber-threats remains a dangerous gap. Security services have warned how smart cities are a prime target for cyber-attacks, highlighting the need to ensure that we design and build these "connected physical environments" properly.[201] Many of the systems and devices integrated into city infrastructure (automated systems, sensors, IoT components and others) are not "secure by design".[202] Just as systems need to be secure by design there is also a recognition that future systems and processes will need to be "resilient by design".[203]

Implementing a comprehensive security-by-design approach in ICT related to urban planning, with enhanced modelling, assessment and planning capabilities for security practitioners and policymakers, would support prevention and protection.

This is through the design, refurbishment and construction of systems, services and spaces that can reduce the threat.

This endorses the need for the UK National Cyber Security Centre's publication on understanding, designing and managing connected places[204] and its 10-step guidance on how organisations can protect themselves in cyberspace.[205]

Many aspects of people's lives in a city are "connected". They depend on digital systems that control sensors, traffic lights, electronic payments, location services, remote-controlled bridges and the monitoring of train tracks etc. The ability to access and convey information also largely depends on digital platforms.

Overall preparedness for accelerating cyber-threats remains a dangerous gap. Security services have warned how smart cities are a prime target for cyber-attacks, highlighting the need to ensure that we design and build these "connected physical environments" properly.[202]

Some systems are regulated by policy or procurement contracts, others are not. What is clear is that, for a city, it is difficult to map out all interdependencies between each system and service. It is even more complex when considering that private enterprises and public services are intertwined in providing different digitally dependent services to the local community.

This morphing and multifaceted landscape presents a challenge because it, again, results in a large increase in cyber-attack vectors.

With cities worldwide racing to adopt technologies that automate services, security researchers have highlighted how many are not doing enough to protect against cyber-attacks. Research suggests that cities vary widely in terms of how prepared they are for possible attacks, often focusing on the functionality of technology rather than security.[206] Researchers who have hacked into city infrastructure to test their security have exposed countless weaknesses. One example was a smart traffic light system that was found without any encryption or authentication, enabling the researcher to feed fake data to their sensors from a drone flying overhead.[207] This, of course, could be fatal in the wrong hands.

Other examples may be an attack on a supply chain[208] or interference with power supply, including through the manipulation of smart meters. Although not caused by malicious intent, a blackout affected the northeast US in August 2003 triggered by a software bug. It resulted in 10 million people without power, secondary incidents and deaths. This also happened in Ukraine in December 2015, when 225,000 customers were affected by a power outage caused by malicious actors that had infiltrated industrial control systems to switch off 30 sub-stations. "The US government has openly acknowledged that Russia has established footholds in their power infrastructures and, in a version of the nuclear mutually assured destruction (MAD) doctrine, have all but admitted that they have the capability to penetrate those of others".[209] Consider how power supply is the backbone of all society's functions. It is essential to the delivery of services and a driver of individual and collective behaviour.[210]

This requires consideration of how intelligence and the monitoring of malicious cyber-activity could be improved across city networks – not only in terms of preventing and intercepting attacks but also in terms of using information and trends to create preventative and protective measures and inform responses to attacks.

Atlanta's computer networks also suffered a cyber-attack that held the city hostage for nearly a week. Reflecting on how this was overcome, the city's former Chief Information Officer noted how "the early efforts involved figuring out what needed to be retired, streamlined, patched and modernised. One of the biggest improvements was to segment the network so hackers couldn't travel from one department's system to another, and add layers of identification requirements".

New policies and procedures for building out new systems were needed, as was a larger security team that now monitors the city's entire network for potential attacks and oversees security for new projects.[211] London's Hackney Council also had its systems paralysed in October 2020 as part of a serious cyber-attack that had real-world impacts for residents.[212]

There is a need for potential cross-system issues between organic and isolated networks such as supervisory control, data acquisition and traffic-management systems to be addressed at a city level.[213]

Likewise, the sheer mass of threat intelligence data available makes it complex to determine and distil what is critical or what is relevant in any given operational environment. The need to find innovative ways to reduce the attack surface and strengthen defence mechanisms is clear. The use of collective intelligence mechanisms to identify dormant components of a threat, which may have compromised network elements to prepare a future attack, would further support this.[214]

This requires consideration of how intelligence and the monitoring of malicious cyber-activity could be improved across city networks – not only in terms of preventing and intercepting attacks but also in terms of using information and trends to create preventative and protective measures and inform responses to attacks. In 2021, New York was reported to be the first city to introduce a real-time cyber-operations centre to share intelligence on, and prepare for, potential cyber-threats,[215] a model that offers a benchmark for other cities.

CASE STUDY
New York City cyber operations centre

On 1 April 2019, the New York County District Attorney's Office, New York City Police Department, New York City Cyber Command and Global Cyber Alliance launched the New York City Cyber Critical Services and Infrastructure (NYC CCSI) Centre. NYC CCSI is a collaboration of professionals from both public and private entities across all sectors of critical infrastructure that unite to combat threats from adversaries globally.

In 2021, New York City became the first major American metropolitan area to open a real-time operational centre to protect against cyber-security threats.[216] NYC CCSI is composed of more than 280 members from 80 organisations across 12 different sectors. The NYC CCSI mission is to share real-time threat information and other relevant data (e.g. indicators of compromise), train jointly and deploy volunteers should an entity or sector require specialist assistance.

To ensure that valuable information is being shared across sectors, NYC CCSI members are in constant communication via a signal channel in which real-time threat intelligence is pushed.

NYC CCSI has held several in-person cyber-training sessions and table-top exercises, where members from across all sectors participate and contribute. These trainings have been held in person at IBM's X-Force Cyber Range in Cambridge, Massachusetts. Within this cyber-training partners share valuable threat intelligence and engage in a series of drills.

The collaboration of the different sectors allows the city to prevent possible cyber-attacks and to be ready should an attack take place.

During the pandemic, NYC CCSI also held a series of discussions with leading security agency partners like the Cybersecurity and Infrastructure Security Agency (CISA) and Palo Alto Networks.

NYC CCSI aims to increase communication and coordination across sectors to protect not only New York City but critical infrastructure across the world through global partners that include but are not limited to Tribunal de Paris, the Liberia Cyber Crime Prevention and Mitigation Agency, Europol, Swiss Federal Department of Justice and the City of London Police.

Case study courtesy of Kenn Kern, Chief Information Officer; Ofelia DeFran, Cyber Security Analyst at New York County District Attorney's Office; and Lieutenant Gustavo Rodriguez of New York Police Department.

This outlines the benefits of establishing a multi-agency, cross-sector, cyber-operations centre and highlights the need for fusion between technical/digital security response and emergency response, as well as the need to recognise and work to resolve the challenges of aligning these disciplines.

This would also offer a platform to consider how public communication campaigns can be harnessed at a city level to support this agenda, as well as investment in the regulation and monitoring of different channels (traditional media, social media or the dark web) and the development of city infrastructure and services that are future-proof.

There is a need to develop integrated arrangements that are accompanied by a set of tools to better assess vulnerabilities in the context of cyber-threats and AI. Moreover, an integrated cyber-risk framework that considers current and future threats, incorporates industry standards, legal and regulatory requirements and management principles would provide cities with a tool for transformation[217] in terms of prevention, protection and preparedness.

Multi-agency preparedness

A cyber-attack can be divided into several phases, with varying levels of activity and impact. Much like an infectious disease outbreak or pandemic, the severity of a cyber-attack may ebb and flow over a protracted period. The diagram below illustrates the phases that may unfold. The action to be taken during each phase, and the partners involved, will depend on how the situation develops over time.[218]

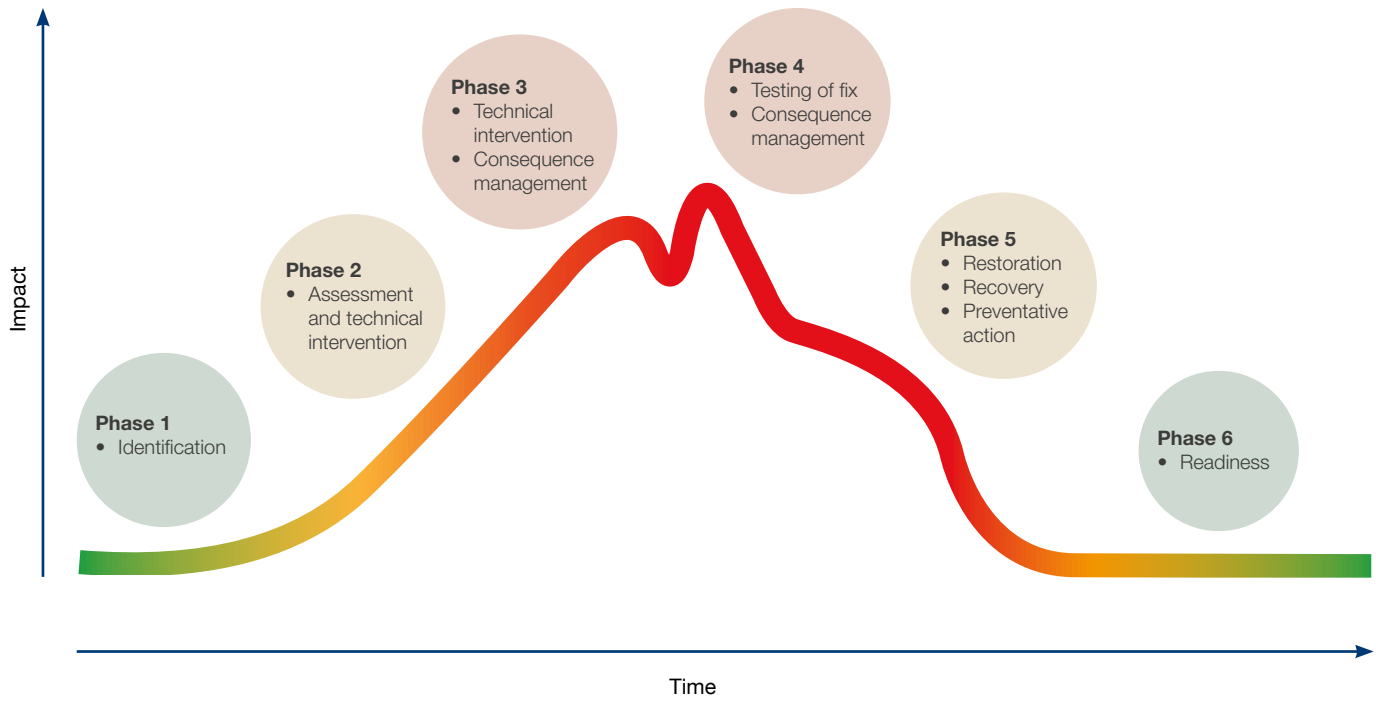
Preparedness for cyber-attacks should also be connected or integrated seamlessly with broader consequence-based planning that sits outside the digital context.

Preparedness will naturally centre on the development of plans, procedures and multi-agency arrangements for responding to the cyber-attack itself, as well as the consequences.

It should also include organised ways to test defensive measures and consider using creative initiatives, such as a hackathon or similar to develop cyber-security further. These types of events are becoming more popular and they promote awareness and collaboration as well as providing a means to expose and address vulnerabilities.

Integrating strong continuity planning that generates the ability to operate without certain digital systems (for example, documenting how decision-making and actions will take place) is crucial in reducing the impact of a cyber-attack. It is likely that some risks are simply too complex to protect against comprehensively, or the protection would be too expensive to build.

The phases of a cyber attack



In those cases, it is important to acknowledge and accept the risk, then focus on a proportionate approach to build overall preparedness to handle and reduce the consequences instead. "The focus should be on testing the capacity to respond to secondary emergencies which are caused by the failure of critical infrastructure."[219]

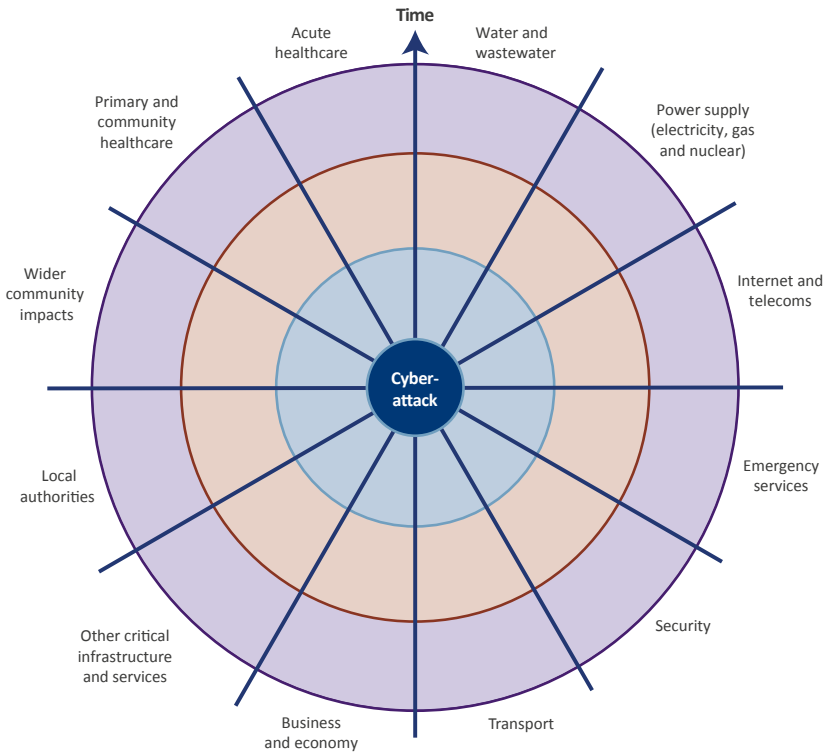
The mapping exercise as detailed in the "Anytown" report by London Resilience could serve as a blueprint to identify ripple effects and the spread of consequences from such an incident.[220]

The "Anytown" model is useful in understanding the potential domino effect upon city systems, notably critical infrastructure interdependencies in generic urban environments. Applying this time-layered and sectorised approach to understanding the cascading effects of a cyber-attack would build in some foresight for planning. "Even if the uncertainty levels of a non-sequential chain of effects remain elevated and hard to predict, the process may help to explore the concurrent, compound and cascading drivers of the escalation process."[221]

Recognising how the initial impact can snowball and lead to other unwanted events and secondary emergencies (in which primary events are less problematic than the chain of effects triggered by their impact[222]) can help to identify vulnerabilities.

Indeed, the principle of preparedness is to understand the threat and its potential consequences in order to ensure the connections, capacity and capability to respond to an attack.

The Anytown model



Practising response in different scenarios is one of the most efficient ways to increase preparedness. This can be done both within organisations and in collaboration with multiple actors locally, regionally and nationally. Training and exercising are critical, yet cyber-based scenarios are few and far between at a multi-agency level. Examples include an executive leadership programme with a module focused on cyber-threats; a laboratory resource used to create large computer networks for use during experiments and exercises in cyber-security,[223] and a significant exercise delivered by the US Army Cyber Institute, which identified a need to improve city responses to cyber-attacks. In this case, the Army Cyber Institute executed a major city, cross-sector exercise in conjunction with Citigroup.

This was the first step in building a framework to prepare, prevent and respond to cyber-attacks on major cities. It included "live-fire" and table-top elements to analyse the capabilities of Charleston, South Carolina, and Savannah, Georgia – two major ports on the US east coast – when confronted with a cyber-attack against their commercial critical infrastructure.[224]

City authorities should consider this type of exercise as part of an annual programme aimed at increasing preparedness. Likewise, at an organisational level, both public and private sector partners should consider how internal training and exercising arrangements could be enhanced. Thames Tideway – considered one of Europe's largest and most complex infrastructure projects – identified the cyber-threat as a priority, delivering an internal exercise to match.

CASE STUDY
Thames Tideway cyber-attack exercise

Following an increase in global ransomware attacks and the UK National Cyber Security Centre's warnings of hostile actors targeting infrastructure providers, Tideway decided to gauge its preparedness for such an event. In November 2019, in collaboration with London Resilience Group, Tideway conducted a crisis-management exercise aimed to test, validate and provide opportunities to develop Tideway's cyber-security defence capabilities. The ransomware scenario was a hybrid minimal-notice exercise.

Meticulous planning ensured that any associated risks were mitigated to minimise disruption to the business. A Tideway service provider for threat monitoring (ThreatSpike Labs) supported the delivery of this exercise, using its software to target individual employees and generate fake ransomware, thus replicating a real-time cyber-attack. The scenario started with a "spear-phishing" campaign, with targeted emails sent to individuals. This was delivered by procuring a domain name that closely matched the Tideway email address that was used to send health and safety alerts.

Once the email and attachment were opened, ThreatSpike used a pre-agreed employee list to deny staff access to the network by "blue-screening" their laptops. As more members of staff opened the email, confusion and panic set in. Information display screens housed on the fifth and sixth floors of the headquarters building began to display a ransomware message demanding £15 million in Bitcoin in return for releasing Tideway systems.

After the initial spear-phishing element, the ransomware injection provided a focus on the very real threat that organisations face. To improve organisational learning, the ransomware attack was combined with an "insider threat", a less understood risk closely associated with cyber-crime, where individuals belonging to an organisation can use their knowledge of the organisation's security and information practices to orchestrate or develop the cyber-attack.

The shock and confusion among staff was clear. The information systems department was soon overwhelmed and just as shocked by the speed of the initial attack. Crisis-management teams were subsequently able to use structured processes to understand the situation, agree priorities and set a strategic direction.

The key learning themes identified were that the business had limited understanding of a ransomware attack and its impact on systems and business continuity. The true impact, financial cost and recovery timescales of such an attack were also misunderstood. The exercise drove discussions on disclosure, how the ransom request should be handled, and which partner agencies to involve. Colleagues from UK Central Government and the Metropolitan Police Service's Cyber Crime Unit also observed the exercise and were able to provide valuable feedback and advice based on real incidents.

Although organisations can never fully protect themselves against cyber-crime, Tideway's commitment to enhancing staff awareness with the existence of robust and practised procedures ensures that the organisation is in the best position to respond to cyber-attacks. The exercise demonstrated that shared understanding and organisational preparedness for such incidents is vital in reducing the recovery time.

Case study courtesy of Thames Tideway, as provided by Charles Frank, Head of Security and Facilities.

Building competence and capabilities through certified training for all levels, regional multi-agency exercises and organisation-specific exercises should be a prerequisite for those with a stake in cyber-preparedness and response. Expert, multi-agency forums can also be effective in increasing awareness and information sharing, consolidating expertise and actions, enhancing resourcing as well as enabling collaborative approaches towards analysis, planning and the handling of cyber-attacks.

The table below summarises some headline considerations in preparedness and response. The list is, of course, not exhaustive but it proposes functions that can be adapted locally to serve as thresholds for preparedness or as "tiers of cyber-resilience". This notion implies a progression of maturity between the tiers, which is theoretically correct but would need to be introduced, tested and evaluated locally.

	Preparedness	Response
1	**Cyber-governance board** The convening of a strategic oversight board to provide the political impetus and investment to drive a coordinated and progressive approach at a senior, cross-sector city level.	**Strategic coordinating group** The senior accountable body, as chaired by the lead agency, which sets the strategy to facilitate collaboration and coordination across multi-agency partners during response.
2	**Infrastructure and resilience strategies** The introduction and/or maintenance of an integrated cyber-risk framework that links with city resilience and infrastructure development strategies to incorporate cyber-security and the consideration of digital dependencies to design out associated risks and threats.	**Strategic and tactical response plans** The activation and application of prepared plans and pre-determined arrangements to guide decision-making, allocate resources and translate strategy into practice. The plans should outline efficient and effective structures to consolidate and discharge multi-agency activity and communications, both in terms of cyber-response and consequence management.
3	**Multi-agency training and exercising** The delivery of a comprehensive training and exercising programme that incorporates both table-top workshops and live simulations. These should include technical exercises designed for intelligence, cyber-experts and investigators to resilience professionals focused on consequence management.	**Consequence management and cyber technical advice cells** The activation of specialist groups to manage specific consequences. For example, humanitarian assistance and psychosocial support, a recovery group or economic impacts committee, etc.

	Preparedness	Response
4	**Cyber-preparedness and foresight group** The development of a focus group that brings together cyber-security experts with cross-sector representatives who understand the potential impact and implications of cyber-attacks. The focus would be horizon scanning, scenario development and consequence mapping to inform preparedness.	**Situational awareness cell** Informed by the real-time situation and the findings of the cyber-security fusion cell, the situational awareness cell is focused on compiling and distilling information to identify and understand the potential consequences of an ongoing cyber-threat/attack. This is with a view to flagging potential problems and solutions while ensuring shared situational awareness.
5	**Cyber-security review committee** A multi-agency steering group that monitors trends, considers the cyber-threat, shares learning from any recent incidents and considers technical security measures and multi-agency arrangements that could be implemented to help reduce vulnerabilities.	**Cyber-security fusion cell** A group of intelligence and cyber-security experts who support the affected organisations, conduct a threat assessment and work to detect hostile actors across multiple platforms. They may also offer the ability to analyse risks with critical dependencies for individuals, organisations and society.
6	**Organisational ICT and business continuity** Assumed to be the baseline position for the majority of public organisations and services. Overseen by a Chief Information Officer, this should include internal governance and continuity plans; investment in expert teams, protective firewalls and suitably robust systems and software; the use of protective marking and restricted access as appropriate; and consistent standards for staff vetting and training.	**Cyber-emergency response team** A specialist team specific to the affected organisation that have the qualifications, experience and expertise to make technical decisions and prioritise reactive measures, such as re-routing, limiting or shutting down systems while enhancing cyber-defences.

Building city resilience

This section has considered the implications of the cyber-threat, notably the concept of cyber-enabled terrorism, on city preparedness. It has sought to progress thinking from the micro perspective of organisation-specific cyber-security to a macro perspective, whereby cities need to drive the pillars of prevention, protection and preparedness collectively and holistically as detailed above. This ranges from the lifecycle management of software and enhancement of ICT security measures to the continuity and protection of critical infrastructure, essential services and city operations, as well as the development of robust multi-agency plans and response arrangements.

It should include a safety net of cyber-insurance provisions to support both the public and private sector in recovering from cyber-attacks and to strengthen the resilience of cities. If a systematic approach to preparedness is applied, it is possible to harness cross-regional or organisational policies and capacities in support of resilience.

Beyond the three pillars discussed there is a need to intensify the education of society. In general, individuals' awareness of the possible consequences of a cyber-attack influences the impact. A social understanding could itself reduce some consequences significantly.

For example, the effects of a cyber-attack would be reduced by people carrying some cash if electronic payment systems stopped working; having alternative transport options if railway systems were disrupted; or by knowing where to obtain information if communication channels failed. The introduction of clear, consistent and authoritative awareness campaigns, the availability of free or subsidised training and a legal responsibility on service providers to inform and protect end users would help this.

Cities need to drive the pillars of prevention, protection and preparedness collectively and holistically as detailed above. This ranges from the lifecycle management of software and enhancement of ICT security measures to the continuity and protection of critical infrastructure, essential services and city operations, as well as the development of robust multi-agency plans and response arrangements.

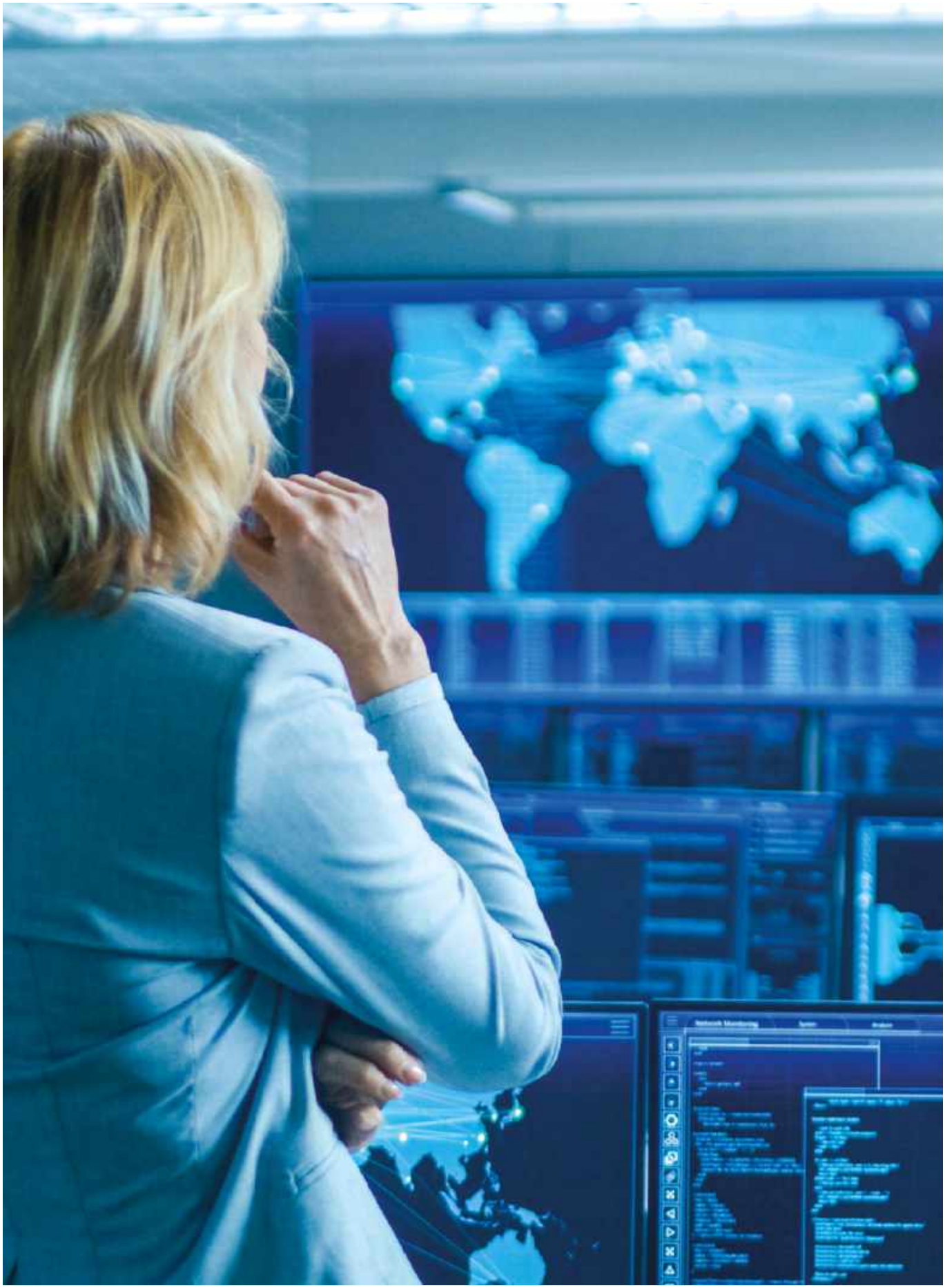
Ultimately, city administrations must prioritise and safeguard the safety, health and economic opportunities of its citizens, and seek to provide an environment rooted in democratic values. The cyber-threat, and especially cyber-enabled terrorism, has the potential to disrupt and undermine all of these. In fact, if over time it materialises more concretely either directly or via crime-as-a-service, it has the potential to significantly impact the very way individuals and communities live their lives. Therefore, a new approach to achieving preparedness is necessary, using many layers of technical, social, collaborative and governing measures across the full attack continuum – before, during and after. This will "necessitate a holistic approach across government and the private sector, driven by cybersecurity and intelligence experts".[225]

Honest and comprehensive capability assessments should be applied internally and across the multi-agency environment to spearhead this agenda. "Leaders must recognise cyber-security and cyber-incident response as a key responsibility and allocate resources to personnel, training and education shortfalls accordingly."[226] Leadership will have to adapt, invest in capacity to change, innovate and pioneer.[227] In this respect, local authorities can have a strong influence on preparedness. The Coalition of City Chief Information Security Officers believes that "local governments can serve as a cornerstone of a nationwide collective defense that brings together cities, counties, states… and the private sector to defend against cyber threats".[228]

This message should be spotlighted. However, it is important to acknowledge that the public sector is constrained by budgets and political priorities. Smaller cities may also be under-resourced and larger ones considered too complex to manage. Therefore, it may be that the most stable approach and most viable long-term strategy to build preparedness and resilience for a city is that local authorities, inhabitants, visitors, commercial businesses and industries have incentives to make cyber-security a priority.

Leadership will have to adapt, invest in capacity to change, innovate and pioneer.[231] In this respect, local authorities can have a strong influence on preparedness.

City leaders will need to provide equitable public services and programmes to help all residents protect themselves, their families and businesses against cyber-threats.[230] Costly security measures are more financially viable and seen as an investment if they are embedded into longer-term strategies, such as those relating to the development of infrastructure. Herein is the force-multiplier effect, harnessed to strike a balance between safety, security and service as part of long-term city development, regeneration and resilience strategies.[230] To quote the motto of the Future of Life Institute, "Technology is giving life the potential to flourish like never before …or to self-destruct. Let's make a difference".[231]



5 Conclusion

> **“Cyberspace has come to underpin almost every aspect of our daily lives, the scale and pervasiveness of cyber ‘insecurity’ is also now recognised as a major concern.”**
>
> United Nations
> *‘UN Secretary-General’s Strategy on New Technologies’*

Resolution 2341 of the UN Security Council on the protection of critical infrastructure against terrorist acts recognised cyber-security as a core priority.[232] In this respect it noted the growing importance of ensuring reliability and resilience of critical infrastructure and its protection from terrorist attacks for national security, public safety and the economy. Indeed, during the seventh review of the UN Global Counter-Terrorism Strategy, Member States expressed “particular concern that terrorist attacks on critical infrastructure could significantly disrupt the functioning of government and the private sector alike and cause knock-on effects beyond the infrastructure sector”. They underlined “the growing importance of protecting critical infrastructure from terrorist attacks and of fostering comprehensive preparedness for such attacks, including through public-private partnership”.[233]

This translates to regional and national agendas as well as the priorities of cities. The digital revolution, arguably accelerated as a side effect of a global pandemic,[234] catapults cities into a new threat environment. This is underpinned by the multifaceted ways in which cyber-capabilities have been used by a range of hostile actors to cause disruption and damage.

As demonstrated, significant cyber-attacks have increased exponentially, while the potential for consequences to cascade out beyond an attack itself and into society with real-world implications is evident. The vulnerabilities and threats identified sound the alarm.

A holistic, action-orientated approach needs to be taken by cities and their constituent authorities to prevent, protect and prepare for cyber-attacks. Cities are essential building blocks for achieving preparedness and resilience at both local and national levels.

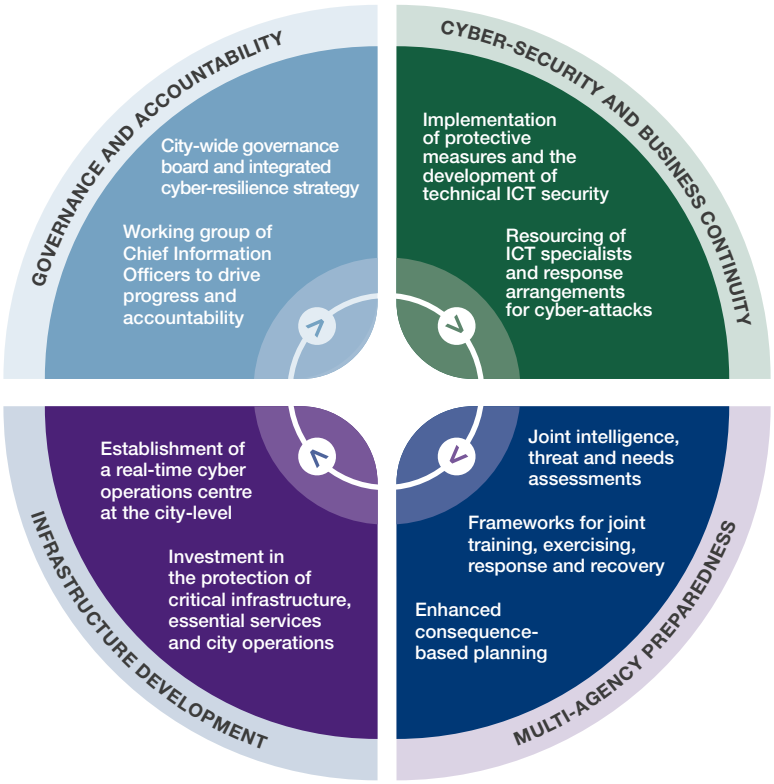
Cyber-attacks and their potential consequences in an urban environment remain a dangerously under-researched issue. In part, this may be because of unresolved questions about definitions and a low threat perception based on an understanding of terrorism that is shaped by physical violence.

These dynamics tend to overshadow the vulnerabilities that city-level systems already face with respect to cyber-attacks that threaten loss of public confidence in authorities, disruption of essential services, interference with social, political and economic activity, and – in their severest expression – physical destruction or harm.

This report has found that a holistic, action-orientated approach needs to be taken by cities and their constituent authorities to prevent, protect and prepare for cyber-attacks.

Cities are essential building blocks for achieving preparedness and resilience at both local and national levels. This is why cyber-security measures need to be applied, enhanced and developed at this level to protect citizens and services.

Overarching components of preparedness for cyber-enabled terrorism



Recommendations

Note: This is an international report designed for an international audience at a city-policy level. It is recognised that arrangements and resources will differ from city to city. It is therefore anticipated and accepted that different recommendations will apply to cities and organisations, subject to context. The implementation of many can be progressed by organisations and/or multi-agency partnerships, whereas others require investment and resource as part of a broader agenda that is appropriately funded as part of city resilience, security and infrastructure development strategies. The approaches of cities should also be harmonised with national approaches to cyber-security and counter terrorism, to ensure city approaches are streamlined against national and international policy.

1	Review the local cyber-threat profile/risk register and work with recognised experts to develop a common understanding of cyber-enabled terrorism and cyber-resilience in order to enable collective progress in this space.
2	Convene a cyber-governance board to ensure that cyber-resilience is embedded into all relevant city strategies and provide the investment, coordination and impetus for action at a senior level.
3	Synchronise strategies to formalise an integrated, action-orientated cyber-security framework. This should consider the development of sound policies and procedures for incorporating cyber-security improvements into the infrastructure-development lifecycle of cities and organisations.
4	Establish a real-time cyber-operations centre at the city level that brings together relevant public and private sector experts to monitor, prepare for and respond to cyber-threats. This should include investment in the physical and mental health of ICT specialists and surge capacity.
5	Enhance outsourcing and contractual arrangements to foster a robust approach towards service delivery and supply-chain resilience, while placing an onus upon providers to protect end users.
6	Ensure relevant standards and procedures for ICT security are being adopted, followed, applied and tested. This should include relevant international standards on information security incident management.[236]
7	Strengthen consequence-based planning assumptions (for example, map the cyber-based threats that could impact critical infrastructure and services to identify the capabilities requiring development).

8	Undertake a cyber-response capability analysis to map resources and identify gaps.
9	Focus on strengthening protective measures (both technical and physical) as well as continuity planning for critical infrastructure to reduce cascading effects.
10	Identify enhancements for multi-agency preparedness, response and recovery structures and arrangements. This should include the development of a cyber-response framework to inform and guide how a cyber-attack is managed and the development of multi-agency capabilities.
11	Intensify cyber-based training and exercising as part of a coordinated programme, utilising “live-fire” and table-top exercises at all levels (national, regional and local multi-agency exercises). This should include the exercising of a variety of system outages and disruptions to critical infrastructure, essential services and city operations.
12	Introduce incentives that stimulate organisations to enhance cyber-security.
13	Invest in ICT, cyber-security and business-continuity expertise and response teams.
14	Strengthen governance, policies and procedures for mitigating and monitoring insider threats.
15	Promote the basic principles of cyber-hygiene and cyber-security and consider implementing these as a mandatory subject in education, delivered to a recognised standard in the relevant country. General cyber-security and awareness communication campaigns should also be pushed into the public domain.
16	Share experience and expertise and take a proactive approach towards building strategic partnerships to bolster cyber-capabilities against current and emerging threats.

6 References

1. United Nations Security Council Counter Terrorism Committee Executive Directorate (CTED) (Unknown). *'Information and Communications Technologies Factsheet'*. (Accessed online).
2. United Nations (2017). Security Council Resolution 2341, p. 2. (Accessed online).
3. United Nations (no date). *'Developments in the Field of Information and Telecommunications in the Context of International Security'*, UN Office of Disarmament Affairs. (Accessed online).
4. United Nations Security Council Counter Terrorism Committee Executive Directorate (CTED) (Unknown). *'Information and Communications Technologies Factsheet'*. (Accessed online).
5. UNOCT (Unknown). *'Cybersecurity'*. (Accessed online).
6. Army Cyber Institute (2021). *'Jack Voltaic 3.0 Cyber Research Report Executive Summary'*. (Accessed online).
7. SecurityInfoWatch (2021). *'By 2026, the 23 billion IoT Connections Will Present New Threat Vectors and Generate $16 billion in IoT Security Revenues.'* (Accessed online).
8. Devasia, Anish (2021). *'IIoT Cyber Attack Vectors and Best Mitigating Practices'*, ControlAutomation (23 July).
9. Hill, S., Creese, S. (2021). *'Why Cyber Resilience Must be a Top-Level Leadership Strategy'*, CAPCO Institute Journal 53: operational resilience (May), p. 82. (Accessed online).
10. Barnard, P. (2020). *'Martyn'*s Law in a Security Convergent World', IFSEC Global. (Accessed online).
11. Fleming, J. (2021). *'GCHQ chief: West Faces "Moment of Reckoning" Over Cybersecurity'*, The Guardian (22 April). (Accessed online).
12. UK Ministry of Defence (2018). *'Global Strategic Trends: The Future Starts Today'*, (sixth edition), pp. 13-18. (Accessed online).
13. United Nations (2018). UN Secretary General's Strategy on New Technologies, pp. 8-9. (Accessed online).
14. ISO (2012). *'ISO/IEC 27032:2012: Information Technology – Security Techniques – Guidelines for Cybersecurity'*. (Accessed online).
15. Interpol (no date). *'Cybercrime'*. (Accessed online).
16. Stock, J. (2021). *'Immediate Action Required to Avoid Ransomware Pandemic'*, Interpol (Accessed online).
17. European Union Agency for Cyber Security (2020). *'Emerging Trends'*. (Accessed online).
18. McGuire, M. (April 2021). *'Nation States, Cyberconflict and the Web of Profit'*, pp. 2-3. (Accessed online).
19. Giannopoulos, G., Smith, H., Theocharidou, M. (2020). *'The Landscape of Hybrid Threats: A conceptual model'*, European Commission, Ispra, p. 28 (Accessed online).
20. McGuire, M. (April 2021). *'Nation States, Cyberconflict and the Web of Profit'*, p. 2. (Accessed online).
21. Ibid. pp. 2-3.
22. McCallum, K. (2021). *'Director General Annual Threat Update'*, UK Security Service MI5. (Accessed online).
23. Kreps, S. (2021). *'Democratizing Harm: Artificial Intelligence in the Hands of Nonstate Actors'*, Brookings Institute, p. 8.
24. Computer Security Resource Centre Glossary (no date). *'Cyber threat'*. (Accessed online).
25. United Nations (2017). Security Council Resolution 2341. (Accessed online).
26. Computer Security Resource Centre (no date). *'Cyber Attack'* definition, National Institute of Standards and Technology. (Accessed online).
27. Lobel-Weiss, N., Gould, T. (2019). London Cyber Incident Response Framework, London Resilience, p. 5.
28. Emery, N.E. (2005). *'The Myth of Cyberterrorism'*, Journal of Information Warfare, 4(1), pp. 80-89.
29. Nelson, B., Choi, R., Iacobucci, M., Mitchell, M., Gagnon, G. (1999). *'Cyberterror: Prospects and Implications'*, Defense Technical Information Center, Fort Belvoir, VA. (Accessed 15 November 2021).
30. Soesanto, S. (2020). *'Cyber Terrorism: Why it exists, why it doesn't*, and why it will', Real Instituto Elcano, (Accessed 15 November 2021).
31. Denning, D.E. *'A View of Cyberterrorism Five Years Later'*, Internet Security: Hacking, Counterhacking, and Society. Edited by K. Himma (Sudbury, MA: Jones and Bartlett Publishers, 2007).
32. Denning, D. (2001). *'Is Cyber-Terror Next?'*, Social Science Research Council. (Accessed online).
33. Nicander, L., Ranstorp, M. (2004). *'Terrorism in the Information Age: New frontiers?'*, Swedish National Defence College.
34. Boholm, M. (2021). *'Twenty-five years of Cyber Threats in the News: A study of Swedish newspaper coverage (1995-2019)'*, Journal of Cybersecurity, 7(1), (Accessed 15 November 2021); Macdonald, S., Jarvis, L., Lavis, S.M. (2019). *'Cyberterrorism Today? Findings from a follow-on survey of researchers'*, Studies in Conflict and Terrorism, (Accessed 15 November 2021); Shandler, R., Gross, M.L., Backhaus, S., Canetti, D. (2021). *'Cyber Terrorism and Public Support for Retaliation – A Multi-Country Survey Experiment'*, British Journal of Political Science, pp. 1-19. (Accessed 15 November 2021); Soesanto, S. (2020). *'Cyber Terrorism'*.
35. Broeders, D., Cristiano, F., Weggemans, D. (2021). *'Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy'*, Studies in Conflict and Terrorism, 0, pp. 1-28. (Accessed 15 November 2021); Conway, M. (2002). *'Reality Bytes: Cyberterrorism and terrorist "use" of the internet'*, First Monday. (Accessed 15 November 2021); Denning, D.E. (2000). Information Warfare and Security (Addison Wesley); Denning, D.E. (2015). *'Rethinking the Cyber Domain and Deterrence'*, Joint Force Quarterly, 77. (Accessed 15 November 2021); Denning, D.E. (2001). *'Activism, Hacktivism, and Cyberterrorism: The internet as a tool for influencing foreign policy'*, Networks and Netwars: The Future of Terror, Crime, and Militancy. Edited by J. Arquilla and D. Ronfeldt (Rand Corporation). (Accessed 15 November 2021); Flemming, P., Stohl, M. (2001). *'Myths and Realities of Cyberterrorism'*,

Countering Terrorism Through International Cooperation. Edited by A.P. Schmid (Vienna: ISPAC), pp. 70-105; Hardy, K., Williams, G. (2014). *'What Is "Cyberterrorism"? Computer and Internet Technology in Legal Definitions of Terrorism'*, Cyberterrorism: Understanding, Assessment, and Response. Edited by T.M. Chen, L. Jarvis and S. Macdonald (New York: Springer, New York) pp. 1-23. (Accessed 15 November 2021); Nelson, B., Choi, R., Iacobucci, M., Mitchell, M., Gagnon, G. (1999). *'Cyberterror: Prospects and Implications'*; Shandler, R. et al. (2021). *'Cyber Terrorism and Public Support for Retaliation'*; Straub, V. J. (2020). *'Beyond Kinetic Harm and Towards a Dynamic Conceptualization of Cyberterrorism'*, Journal of Information Warfare, 20(3).

36. Egloff, F. (2021). *'Intentions and Cyberterrorism'*, The Oxford Handbook of Cyber Security.
37. Dunn Cavelty, M. (2008). *'Cyber-Terror – Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate'*, Journal of Information Technology and Politics, 4(1), pp. 19-36. (Accessed 15 November 2021); Soesanto, S. (2020). *'Cyber Terrorism'*; Weimann, G. (2004). *'Cyberterrorism How Real Is the Threat?'*, United States Institute of Peace.
38. Soesanto, S. (2020). *'Cyber Terrorism'*.
39. Macdonald, Jarvis and Lavis (2019). *'Cyberterrorism Today?'*.
40. McKune, S., Hilts, A. (2015). *'An Analysis of the International Code of Conduct for Information Security'*, Citizen Lab. (Accessed online).
41. Straub (2020). *'Beyond Kinetic Harm'*.
42. Broeders, D., Cristiano, F., Weggemans, D. (2021). *'Too Close for Comfort'*; Hardy, K., Williams, G. (2014). *'What Is "Cyberterrorism"?'*.
43. Soare, S.R., Burton, J. (2020). *'Smart Cities, Cyber Warfare and Social Disorder'*, NATO CCDCOE. (Accessed online).
44. Pelton, J., Singh, I. (2019). *'How Nations and Smart Cities Can Cope with Cyber-Terrorism and Warfare'*, Smart Cities of Today and Tomorrow: Better Technology, Infrastructure and Security, (Springer International Publishing).
45. UK Government (2016). *'National Cyber Security Strategy 2016-2021'*, p. 20. (Accessed online).
46. Hill and Creese. *'Why Cyber Resilience Must be a Top-Level Leadership Strategy'*, p. 80. (Accessed online).
47. Brooks, C. (2021) *'Alarming Cybersecurity Stats'*, Forbes.com (2 March). (Accessed online).
48. Newburger, E. (2021). *'Ransomware Attack Forces Shutdown of Largest Fuel Pipeline in the U.S.'*, CNBC (9 May). (Accessed online).
49. BBC (2021). *'Hacker Tries to Poison Water Supply of Florida Cty'*, (8 February). (Accessed online).
50. BBC (2021). *'Swedish Coop Supermarkets Shut Due to US Ransomware Cyber-Attack'*, (3 July). (Accessed online).
51. Menn, J., Bing, C. (2021). *'EXCLUSIVE Governments Turn Tables on Ransomware Gang REvil by Pushing It Offline'*, Reuters. (Accessed online).
52. Centre for Strategic and International Studies. *'Significant Cyber Incidents'*. (Accessed online).
53. European Union Agency for Cyber Security (2020). *'Main Incidents in the EU and Worldwide'*. (Accessed online).
54. Rushe, D., Borger, J. (2021). *'Age of the Cyber-Attack: US struggles to curb rise of digital destabilization'*, The Observer (14 June). (Accessed online).
55. Bing, C. (2021). *'Exclusive: U.S. to Give Ransomware Hacks Similar Priority as Terrorism'*, Reuters. (Accessed online).
56. UNOCT (2021). *'Counter Terrorism Online with Artificial Intelligence: A joint report by UNICRI and UNCCT'*, p. 5.
57. Starks, T. (2021). *'Facebook Tackles Hacking Groups with Apparent Ties to Palestine, Hamas'*, CyberCcoop. (Accessed online).
58. Hymas, C. (2019). *'ISIL Terrorists Hack Ordinary Peoples'* Dormant Twitter Accounts', The Telegraph (18 November). (Accessed online).
59. UNOCT (2021). *'Algorithms and Terrorism: The malicious use of artificial intelligence for terrorist purposes. A Joint Report by UNICRI and UNCCT'*, pp. 17-18. (Accessed online).
60. Kreps (2021). *'Democratizing Harm'*, pp. 8-9.
61. Egloff, F. (2021). *'Intentions and Cyberterrorism'*.
62. Greenberg, A. (2020). *'ISIS Allegedly Ran a Covid-19 PPE Scam Site'*. (Accessed online).
63. US Department of Justice (2020). *'Global Disruption of Three Terror Finance Cyber-Enabled Campaigns: Largest ever seizure of terrorist organizations'* cryptocurrency accounts'. (Accessed online).
64. Finklea, K. (2017). *'Dark Web, Congressional Research Service Paper'*, p. 1. (Accessed online).
65. UNOCT (2021). *'Algorithms and Terrorism'*, p. 5. (Accessed online).
66. Ibid, p. 5.
67. US Department of Justice (2012). *'Assistant Attorney General for National Security Lisa Monaco Speaks at the "2012 Cybercrime Conference"'*. (Accessed online).
68. Flashpoint (2017). *'Cyber Jihadists Dabble in DDoS: Assessing the threat'*. (Accessed online).
69. Europol (2021). *'European Union Terrorism Situation and Trend report'*, p. 105. (Accessed online).
70. UNOCT (2021). *'Algorithms and Terrorism'*, p. 27. (Accessed online).
71. Europol (2021). *'European Union Terrorism Situation and Trend report'*, p. 59. (Accessed online).
72. Department of Energy (2021). *'Biden Administration Takes Bold Action to Protect Electricity Operations from Increasing Cyber Threats'*. (Accessed online).

6 References
continued

73. UK Government (2020). *'New Telecoms Security Law to Protect UK from Cyber Threats'*. (Accessed online).
74. UK Government (2021). *'Global Britain in a Competitive Age: The integrated review of security, defence, development and foreign policy'*. (Accessed online).
75. Cabinet Office (2021). *'National Cyber Strategy 2022'*. (Accessed online).
76. National Cyber Security Centre (2018). *'New Cyber Attack Categorisation System to Improve UK Response to Incidents'*. (Accessed online).
77. Lobel-Weiss and Gould. *'London Cyber Incident Response Framework'*, pp. 5-6.
78. Cyber Security and Infrastructure Security Agency (2021). Infrastructure Resilience Planning Framework, Version 1.0., p. 20. (Accessed online).
79. Colonial Pipeline (2021). *'Media Statement: Colonial Pipeline Disruption'*,Colpipe.com (8 May). (Accessed online); Wilkie, C. (2021). *'Colonial Pipeline Paid $5 million Ransom One Day After Cyberattack, CEO Tells Senate'*, CNBC, (8 June). (Accessed online); Osborne, C. (2021). *'Colonial Pipeline Attack: Everything you need to know'*, ZDNet (13 May). (Accessed online).
80. Krauss, C. et al. (2021). *'Gas Pipeline Hack Leads to Panic Buying in the Southeast'*, The New York Times (11 May). (Accessed online)
81. Ralston, W, (2020). *'The Untold Story of a Cyberattack, a Hospital and a Dying Woman'*, Wired (11 November). (Accessed online).
82. Ibid.
83. BBC (2017). *'Cyber-attack: Europol Says It Was Unprecedented in Scale'*. (Accessed online).
84. CNBC (2017). *'Unprecedented Cyber-Attack Hits 200,000 in At Least 150 Countries, and the Threat Is Escalating'*. (Accessed online).
85. NHS England (2018). *'Lessons Learned Review of the WannaCry Ransomware Cyber Attack'*. (Accessed online).
86. Kroustek, J. (2017). *'WannaCry update: The worst ransomware outbreak in history'*. (Accessed online).
87. Larson, S. (2017). *'Massive cyberattack targeting 99 countries causes sweeping havoc'*. CNN. (Accessed online).
88. National Audit Office. *'Investigation: WannaCry cyber-attack and the NHS'*. (Accessed online).
89. Ibid.
90. UK Government. (2018) *'Securing Cyber Resilience in Health and Care: October 2018 update'*. (Accessed online).
91. NHS England (2018). *'Lessons Learned Review of the WannaCry Ransomware Cyber Attack'*. (Accessed online).
92. NHS Digital. Cyber Incident Response Exercise (CIRE). (Accessed online).
93. NHS England (2018). *'Lessons Learned Review of the WannaCry Ransomware Cyber Attack'*. (Accessed online).
94. UK Government (2019). *'Securing Cyber Resilience in Health and Care: Progress update 2019'*. (Accessed online).
95. CBC (2021). *'Toronto Transit System Hit by Ransomware Attack, TTC Says No Significant Disruptions'*, The Canadian Press (29 October). (Accessed online); CBC (2021). *'TTC CEO Apologizes in the Wake of Ransomware Attack'*, CBC News (5 November). (Accessed online).
96. CBC (2021). *'Up to 25,000 TTC Employees'* Personal Information May Have Been Stolen in Cyber-Attack, Agency Says', CBC News (8 November). (Accessed online).
97. Cybersecurity and Infrastructure Security Agency (no date). *'Critical Infrastructure Sectors'*. (Accessed online).
98. Livingstone, D., Lewis, P. (2016). *'Space, the Final Frontier for Cybersecurity?'*, Chatham House, p. 2. (Accessed online).
99. Livingstone and Lewis. *'Space, the Final Frontier for Cybersecurity?'*, p.6. (Accessed online).
100. Pescaroli, G. et al (2018). *'Increasing Resilience to Cascading Events: The M.OR.D.OR. scenario'*, Safety Science 110(C), Elsevier, p. 134. (Accessed online).
101. Theohary, C. A., Rollins, J. W (2015). *'Cyberwarfare and Cyberterrorism: In Brief'*, Congressional Research Service 7-5700, www.crs.gov R43955 (27 March). (Accessed online).
102. Yunos, Z., Sulaman, S., (2017). *'Understanding Cyber Terrorism from Motivational Perspectives'*, Journal of Information Warfare 16(4), pp. 1-13. (Accessed online).
103. United Nations and Interpol (2018). *'The Protection of Critical Infrastructures Against Terrorist Attacks: Compendium of good practices'*. (Accessed online).
104. United Nations Security Council Counter Terrorism Committee Executive Directorate (CTED) (no date). *'Information and Communications Technologies Factsheet'*. (Accessed online).
105. Darknet Diaries (2021). *'EP 96: The police station incident'*. (Accessed online).
106. Ibid.
107. Dellinger, A. J. (2021). *'Distributed Denial of Secrets Is Picking Up Where Wikileaks Left Off'*, Mic.com (21 October). (Accessed online).
108. Greenberg, A. (2020). *'Hack Brief: Anonymous Stole and Leaked a Megatrove of Police Documents'*, Wired (22 June). (Accessed online).
109. Ibid.
110. Brian Krebs (2020). *'"BlueLeaks" Exposes Files from Hundreds of Police Departments'*, KrebsOnSecurity (22 June). (Accessed online).
111. Ibid.
112. Lee, M. (2020). *'Law Enforcement Websites Hit by BlueLeaks May Have Been Easy to Hack'*, The Intercept (19 August). (Accessed online).

113. Chenetz, M. (2021). *'Log4j Developer Response'*, Cisco Blogs (10 December). (Accessed online).

114. Hay Newman, L. (2021). *'The Log4J Vulnerability Will Haunt the Internet for Years'*, Wired (13 December). (Accessed online).

115. Cimpanu, C. (2021). *'New Moses Staff Group Targets Israeli Organizations in Destructive Attacks'*, The Record (15 November). (Accessed online).

116. Check Point (2021). *'Uncovering MosesStaff Techniques: Ideology over Money'* (15 November). (Accessed online).

117. Ibid.

118. Twitter (2021). @Moses_staff_se. (Accessed online).

119. ISWNews (2021). *'Disclosure of Israeli Military Secret Information! +File'*, (14 November). (Accessed online).

120. Hay Newman, L. (2021). *'DarkSide Ransomware Hit Colonial Pipeline – and Created an Unholy Mess'*, Wired (10 May). (Accessed online); Welt (2021). 'Zerstörte Autos, Sabotage – das wird es nächsten Sommer auf jeden Fall geben'. (22 November). (Accessed online).

121. Bergman, R. (2021). *'Mysterious Hacker Group Suspected in July Cyberattack on Iranian Trains'*, The New York Times (14 August). (Accessed online); Cimpanu, C. (2021). *'Cyber-Attack on Iranian Railway was a Wiper Incident, Not Ransomware'*, The Record (29 July). (Accessed online).

122. Tsai, O. (2021). *'A New Attack Surface on MS Exchange Part 1 - ProxyLogon!'*, Blog.orange.tw (6 August). (Accessed online).

123. Microsoft (2021). *'HAFNIUM Targeting Exchange Servers with 0-day Exploits'*. (Accessed online); The White House (2021). *'The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People'*s Republic of China', Whitehouse.org (19 July). (Accessed online).

124. Tsai. *'A New Attack Surface'*.

125. Gallagher, S., MacKenzie, P. (2021). *'Conti Affiliates use ProxyShell Exchange Exploit in Ransomware Attacks'*, Sophos News. (Accessed online).

126. Barrett, B. (2021). *'The FBI Takes a Drastic Step to Fight China'*s Hacking Spree', Wired (14 April). (Accessed online).

127. Faou, M. et al. (2021). *'Exchange Servers Under Siege from at Least 10 APT Groups'*, ESET (10 March). (Accessed online).

128. Gallagher, S., Mackenzie, P. *'Conti affiliates use ProxyShell Exchange'*; O'Donnell-Welch, L. (2021). *'Vulnerable Microsoft Exchange Servers Hit with Babuk Ransomware'*, Duo.com (4 November). (Accessed online).

129. CERT Luxembourg (2021). *'TR-64 – Exploited Exchange Servers – Mails with links to malware from known/valid senders'*, Circl.lu (10 November). (Accessed online); Kenefick, I., Kropotov, V. (2021). *'QAKBOT Loader Returns With New Techniques and Tools'*, TrendMicro (13 November). (Accessed online).

130. Twitter (2021). @GossiTheDog (1 November). (Accessed online); Fahmy, M. et al. (2021). *'Squirrelwaffle Exploits ProxyShell and ProxyLogon to Hijack Email Chains'*, TrendMicro (19 November). (Accessed online).

131. Ibid.

132. CERT Luxembourg (2021). *'TR-64 - Exploited Exchange Servers'*.

133. Tsai. *'A New Attack Surface'*.

134. (2020). *'Antwerp Laboratory Becomes Latest Victim of Cyber-Attack'*, The Brussels Times (29 December). (Accessed 26 November 2021).

135. (2020)..'Antwerps laboratorium doelwit van ransomware', Computable (29 December). (Accessed 26 November 2021).

136. AN.11.LB.145433/2020 dd. 28/12/2020

137. (2021). *'Cyberaanval tegen nog enkele labo'*s: *'Mogelijke verstoring vaccinatiecampagne'*, DataNews (8 January) (Accessed 26 November 2021).

138. (2020). *'Ransomware-aanval verandert mentaliteit bedrijven'*, Computable (15 October). (Accessed 26 November 2021).

139. (2021). *'Drie tactieken om ransomware-aanvallen tegen te gaan'*, Techzine (11 November). (Accessed 26 November 2021).

140. Europees Parlement (2021). *'Hoe het Parlement cyberveiligheid in de EU wil verbeteren (interview)'*, (16 November). (Accessed 26 November 2021).

141. Chaudhury, D. (2020). *'Ransomware Is Taking a Psychological Toll on Cyber Security Experts'*, ITSecurity Wire, (3 November). (Accessed online); Collier, K. (2021). *'Barely Able to Keep Up: America'*s cyberwarriors are spread thin by attacks', NBC News (8 July). (Accessed online); Palmer, D. (2021). *'Ransomware Attacks Against Hospitals Are Having Some Very Grim Consequences'*, ZDNet (29 September). (Accessed online); Ranger, S. (2020). *'"The Most Stressful Four Hours of My Career": How it feels to be the victim of a hacking attack'*, ZDNet (26 June). (Accessed online).

142. Wilkie, C. (2021). *'Colonial Pipeline Paid $5 million Ransom One Day After Cyberattack, CEO tells Senate'*, CNBC (8 June). (Accessed online).

143. Ranger. '"The Most Stressful Four Hours of My Career".

144. Cundy, A. (2021). *'"Cyber Trauma" Leaves Online Victims with Psychological Scars'*, Financial Times (26 January). (Accessed online); Kamkar, K, Duquette, R. (2021). *'Psychological Trauma and Cybercrime'*, Canadian Occupational Safety (16 April). (Accessed online); *'The Psychology of Cybercrime – 3.1 Impact of Cybercrime on Victims and Coping Strategies'* Open.edu. (Accessed online).

145. Guynn, J. (2020). *'Anxiety, Depression and PTSD: The hidden epidemic of data breaches and cyber crimes'*, USA Today (21 February). (Accessed online).

6 References
continued

146. Lamont, T. (2016). *'Life After the Ashley Madison Affair'*, The Guardian (28 February). (Accessed online); Ralston, W. (2021). *'They Told Their Therapists Everything. Hackers Leaked It All'*, Wired (4 May). (Accessed online).

147. Hinkley, C. (2019). *'Preventing PTSD and Burnout for Cybersecurity Professionals'*, DarkReading (16 September). (Accessed online).

148. Robinson, C. (2021). *'In Cybersecurity Every Alert Matters'*, IDC (October). (Accessed online); Triolo, C. (2021). *'Avoid Fear of Missing Incidents with Automation and XDR'*, FireEye (16 February). (Accessed online); Morris, A. (2021). *'Cybersecurity Alert Fatigue: Why It Happens, Why It Sucks, and What We Can Do About It'*, IOActive (9 June). (Accessed online).

149. Richmond, C. et al. (2021). *'The Voice of the Analysts – Improving Security Operations Center Processes Through Advanced Technologies'*, IDC and FireEye (January). (Accessed online).

150. Robinson, C. (2021). *'In Cybersecurity Every Alert Matters'*, p. 6.

151. Microsoft (2021). *'Decoding NOBELIUM: The Docuseries – Episode 4 After-Action Report'*. (Accessed online).

152. Bulut, U., Frye, E., Greene, J., Li, Y., Lee, M., (2020). *'The Hidden Price of Convenience: A Cyber-Inclusive Cost-Benefit Analysis of Smart Cities'*, Research in Mathematics and Public Policy. Edited by M. Lee and A. Najera Chesler (Springer International Publishing) pp. 81-92; Soare and Burton (2020). *'Smart Cities'*; Soesanto, S. (2020). *'Cyber Terrorism'*.

153. Crelier. *'Trend Analysis'*; Soare and Burton. *'Smart Cities'*.

154. Pelton and Singh. *'How Nations and Smart Cities Can Cope'*.

155. Kreps. *'Democratizing Harm'*, pp. 1-4.

156. Warrick, J. (2017). *'Use of Weaponized Drones by ISIS Spurs Terrorism Fears'*, Washington Post. (Accessed online).

157. Kreps. 'Democratizing Harm, p. 1.

158. Ibid pp. 2-4.

159. Bloomberg, J. (2017). *'This Is Why Quantum Computing Is More Dangerous Than You Realize'*, Forbes (11 August). (Accessed online).

160. Herman, A.. (2018). *'Winning the Race in Quantum Computing'*, Hudson Institute (21 May). (Accessed online).

161. (2018) *'Russia Wants to Build a Quantum Computer in Five Years'*, Russia Business Today (5 March). (Accessed online).

162. NIST (no date). *'Post Quantum Cryptography'*, NIST Computer Security Resource Center. (Accessed online).

163. Kreps. *'Democratizing Harm'* p. 9.

164. UNOCT. *'Algorithms and Terrorism'*.

165. Ibid. p. 33.

166. Lima, A. et al. (2016). *'Towards Safe and Secure Autonomous and Cooperative Vehicle Ecosystems'*, Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy.

167. Microsoft (2021). Microsoft Digital Defense Report,, (October).

168. Sagduyu, Y. et al. (2021). *'Adversarial Machine Learning for 5G Communications Security.'* ArXiv, Cornell University (7 January). (Accessed online).

169. Townsend-Drake, A., Harvin, D., Sellwood, C. (2021). *'Bioterrorism: Applying the Lens of COVID-19'*, Counter Terrorism Preparedness Network, p. 28.

170. UNOCT. *'Algorithms and Terrorism'*, p. 35.

171. Mueller, S. (2020). *'Facing the 2020 Pandemic: What does cyberbiosecurity want us to know to safeguard the future?'*, Science Direct 3(1), Elsevier.

172. Puzis, R. et al. (2020). *'Increased Cyber-Biosecurity for DNA Synthesis'*, Nature Biotechnology 38(12), pp. 1379-1381. (Accessed online).

173. Warmbrod, K. L., Revill, J., Connell. N. (2020). *'Advances in Science and Technology in the Life Sciences: Implications for biosecurity and arms control'*, United Nations Institute for Disarmament Research. Geneva, Switzerland.

174. Doubleday, J. (2021). *'Cyber Improvements Could Lead to More Insider Targeting, Intel Official Says'*, Federal News Network (5 October). (Accessed online).

175. (2020). *'Report Insider Threats Rise by 47% in Two Years'*, CISO MAG (28 April). (Accessed online).

176. Swann, S. (2011). *'Rajib Karim: The terrorist inside British Airways'*, BBC. (Accessed online).

177. Kreps. *'Democratizing Harm'*, p. 4.

178. Seffers, G. (2017). *'Virtual Reality a Friend And Foe in Terror Fight'*, Signal Magazine (1 June). (Accessed online).

179. Fortune Business Insights (2021). *'Virtual Reality (VR) Market to Reach USD 84.09 Billion by 2028; Acquisition of NextVR by Apple Inc. to Incite Business Development: Fortune Business InsightsTM'*, GlobeNewswire News Room (19 August). (Accessed online).

180. Silver, N. *'Pokemon Go Warnings – Will They Work?'*. (Accessed online).

181. Chen, P.L. et al. (2018). *'Pokemon Gaming Causes Pedestrians to Run a Red Light: An observational study of crossing behaviours at a signalised intersection in Taipei City'*, ScienceDirect. (Accessed online).

182. Graells-Garrido, E., Ferres, L., Bravo, L., Caro, D. (2016). *'The Effect of Pokémon Go on The Pulse of the City: A Natural Experiment'*, EPJ Data Science. (Accessed online).

183. UNOCT. *'Algorithms and Terrorism'*.

184. Kreps. *'Democratizing Harm'*, p. 1.

185. Ibid, p. 3.

186. UN Habitat (no date) *'What is a City?'* Accessed Online.

187. Pandy, P. et al. *'Making Smart Cities Cybersecure: Ways to address distinct risks in an increasingly connected urban future'*, Deloitte, pp. 4-7. (Accessed online).

188. Poon, L. (2021). *'What It Will Take to Protect Cities Against Cyber Threats'*, Bloomberg CityLab. (Accessed online).

189. PWC (TBC). *'Cyber Security Strategy 2022: Responding to the Ransomware Threat'*. (Accessed online).

190. BSI (no date). *'Cybersecurity Standards'*. (Accessed online).

191. UK Government (2020). *'Cyber Security Guidance'*, National Cyber Security Centre. (Accessed online).

192. Petersen, R. et al (2020). *'Workforce Framework for Cybersecurity (NICE Framework)'*, National Institute of Standards and Technology. (Accessed online).

193. Feller, G. *'Protecting Our Cities from Cyber Attacks'*, Meeting of the Minds. (Accessed online).

194. European Union Agency for Cybersecurity (2021). NIS Directive. (Accessed online).

195. Army Cyber Institute. *'Jack Voltaic 3.0'*, p. 8.

196. Hill and Creese. *'Why Cyber Resilience Must Be a Top-Level Leadership Strategy'*, p. 8.

197. City of Stockholm – STOKAB (2021). *'Our role in Stockholm'*. (Accessed online).

198. NetNod (no date). *'Rock Solid Internet Infrastructure'*. (Accessed online).

199. Mayor of London (2018). *'Smarter London Together: The Mayor'*s roadmap to transform London into the smartest city in the world', Greater London Authority. (Accessed online).

200. Mayor of London (2020). *'London City Resilience Strategy'*, Greater London Authority, pp. 51-53.

201. Corera, G. (2021). *'Spy Bosses Warn of Cyber-Attacks on Smart Cities'*, BBC. (Accessed online).

202. Crelier, A. (2019). *'Trend Analysis: The Challenges of Scaling the Internet of Things'*, Center for Security Studies. (Accessed online); DCMS (2019). *'Secure by Design'*. (Accessed online).

203. Hill and Creese. *'Why Cyber Resilience Must Be a Top-Level Leadership Strategy'*, p. 83.

204. UK Government (2021). *'Connected Places: Cyber Security Principles'*, NCSC. (Accessed online).

205. National Cyber Security Centre (2021). *'10 Steps to Cyber Security'*. (Accessed online).

206. Wong, S. (2015). *'Cyber Attack: How easy is it to take out a smart city?'*, New Scientist. (Available online).

207. Ibid.

208. ENISA (2021). *'ENISA Threat Landscape for Supply Chain Attacks'*, European Union Agency for Cyber Security. (Accessed online).

209. Hill and Creese. *'Why Cyber Resilience Must Be a Top-Level Leadership Strategy'*, p. 81.

210. Pescaroli, G., Turner, S., Gould, T., Alexander, D., Wicks, R. (2017). *'Cascading Impacts and Escalations in Wide-Area Power Failures'*, UCL IRDR and London Resilience Special Report 2017-01, Institute for Risk and Disaster Reduction, University College London, p. 4.

211. Poon, L. (2021). *'What It Will Take to Protect Cities Against Cyber Threats'*, Bloomberg CityLab. (Accessed online).

212. BBC (2021). Cyber attack: Hackers post Hackney Council's *'stolen documents'*. (Accessed online).

213. Army Cyber Institute. *'Jack Voltaic 3.0'*, p. 7.

214. Hogan, M. (2013). "Anytown: Final Report", London Resilience, p. 4. (Accessed online).

215. The Wall Street Journal (2021). *'New York City Opens Cyberattack Defense Centre'*, (Accessed online).

216. Ibid.

217. Pandy, P. et al. *'Making Smart Cities Cybersecure'*, p. 9.

218. Lobel-Weiss and Gould. *'London Cyber Incident Response Framework'*.

219. Pescaroli et al. *'Increasing Resilience to Cascading Events'*, p. 138.

220. Hogan. *'Anytown: Final Report'*.

221. Pescaroli et al. *'Increasing Resilience to Cascading Events'*, p. 134.

222. Ibid. p. 131.

223. Swedish Defence Research Agency (2021). CRATE – Cyber Range And Training Environment. (Accessed online).

224. Army Cyber Institute. *'Jack Voltaic 3.0'*, p. 1.

225. Hill and Creese. *'Why Cyber Resilience Must Be a Top-Level Leadership Strategy'*, p. 83..

226. Army Cyber Institute. *'Jack Voltaic 3.0'*, p. 9.

227. Hill and Creese. *'Why Cyber Resilience Must Be a Top-Level Leadership Strategy'*, p. 83.

228. Coalition of City CISCO's (2021). *'Objective: Collective Defense'*. (Accessed online).

229. Ibid.

230. Townsend-Drake, Harvin and Sellwood. *'Bioterrorism'*, p. 57.

231. Future of Life Institute. (Accessed online).

232. United Nations (2017). Security Council Resolution 2341.

233. United Nations (2021). *'The United Nations Global Counter-Terrorism Strategy: Seventh Review'*. (Accessed online).

234. European Union Agency for Cyber Security (2020). *'The Year in Review,'* p. 8. (Accessed online).

235. ISO/IEC 27035-1:2016. *'Information Technology – Security Techniques – Information Security Incident Management – Part 1: Principles of incident management'*. (Accessed online).

CTPN
COUNTER TERRORISM
PREPAREDNESS NETWORK