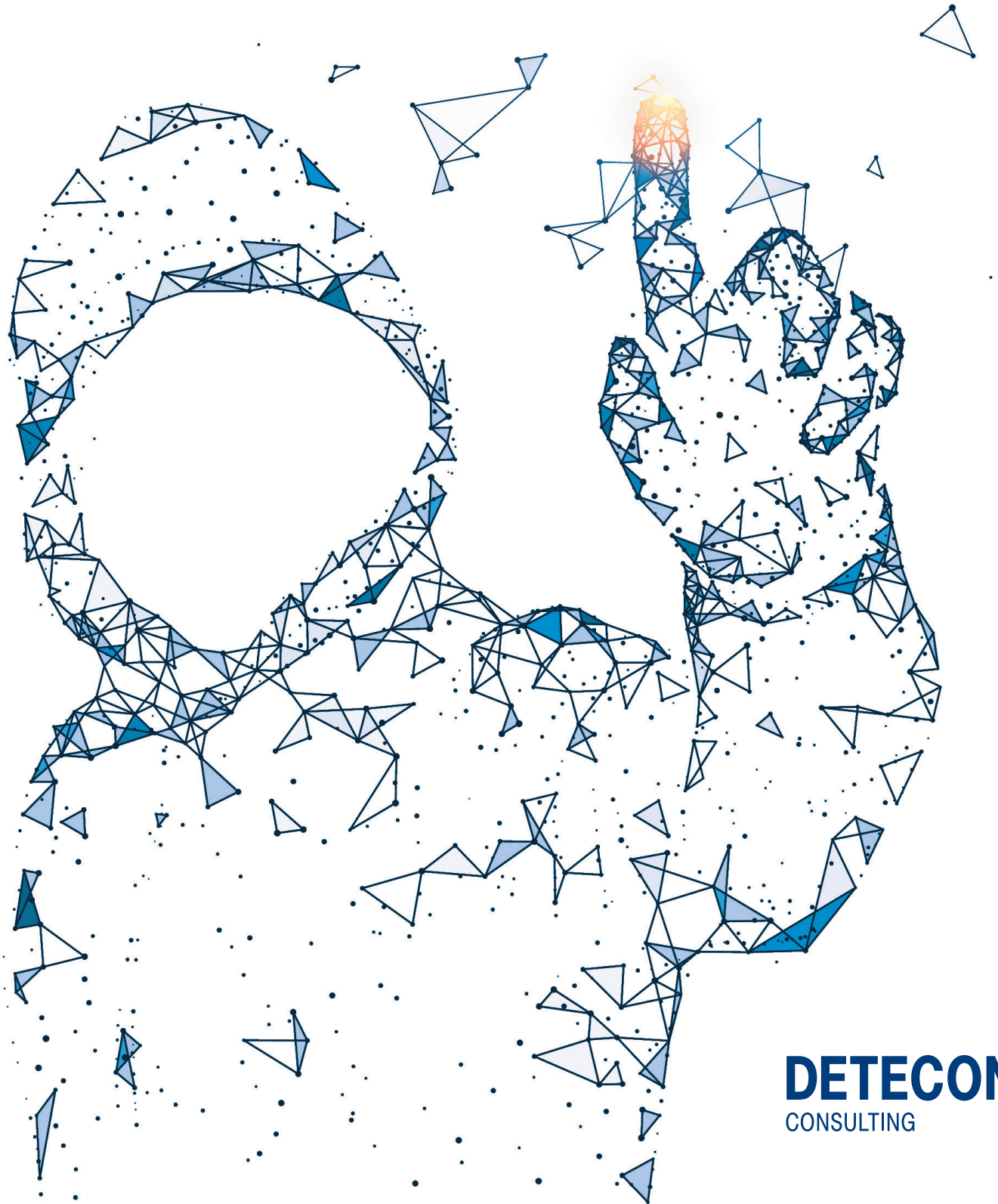
OPINION PAPER

Cybersecurity

New Challenges and Effective Defence



DETECON
CONSULTING

Content

The New Cyber Environment	3
Expanding Attack Surface	5
Trends in the Threat Landscape	6
Effective Cyber Defence	12
Trends in Defence Tools and Tactics	13
The New Defenders	14
Next-generation Security Operations Centres (SOCs)	15
A Perspective from Detecon's Cybersecurity Experts	17
Authors	18
Company Profil	19
Footnotes	19 - 20

Cybersecurity

Today's cybersecurity is a continuous battle to retain control over devices and data, all while navigating key relationships across a rapidly expanding attack surface that extends beyond boundaries and borders. While their basic modus operandi may not have changed much in a decade, while the tools and vectors for cybercrime currently enjoy a scale advantage in costs, reach and damage. The task of cyber defence is to reduce that advantage.

Cybersecurity legislation and sectoral guidelines are rapidly creating the foundations for international cyber laws – but the burden of responsibility to protect data and assets falls largely on companies. For companies of any size, in any sector, effective cybersecurity only succeeds where a strong foundation of the right people, skills and technology work together to protect core knowledge and assets.

The New Cyber Environment

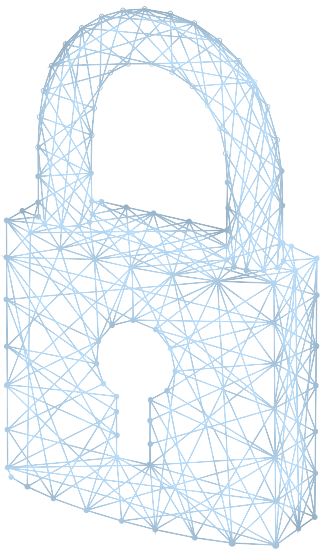
Cybersecurity describes the activities and technologies that collectively defend the assets and interests of an organisation (or a nation state) in cyberspace. Valued at approximately €100 billion in 2017[1] and predicted to grow by 12-13% annually to 2020, the global civil and military cybersecurity business includes the operations, tactics, network systems, software, algorithms and devices that protect organisations against security breaches, data theft and sabotage of computer networks.

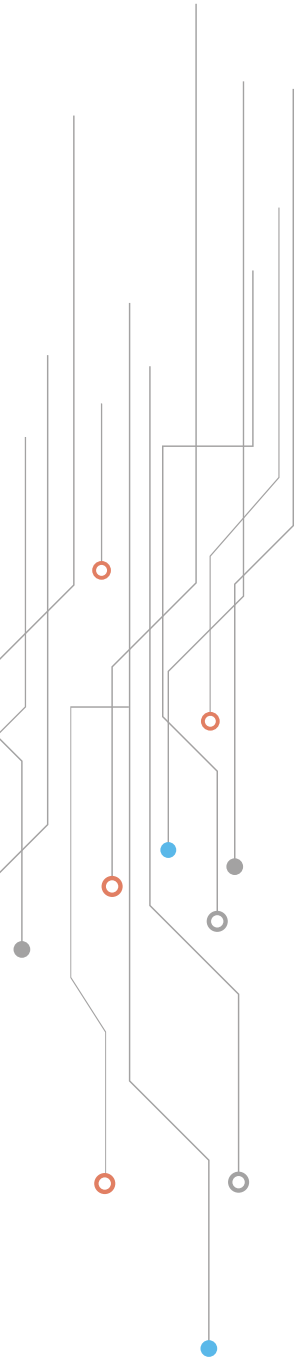
Cyberspace is core to enabling business as usual (e.g. in the European Commission Digital single market) across the connected global economy, comprising of public and private networks, the surface and dark web, cloud storage, Industrial Control Systems (ICS) and Internet of Things (IoT). Any system or device that is connected to the internet, or otherwise exposed to connection (including sensors, mobile and data storage devices) is vulnerable to exploitation and attack.

In 2017 the cost of cybercrime to the global economy was approximately €370 billion[2]; by early 2018, estimates placed total losses at almost €485 billion – one percent of global GDP[3]. We see an increase in spending on cybersecurity, as organisations become aware of the costs and risks associated with ignoring growing, pervasive threats. Cyber is increasingly recognized as a corporate risk, treated at board and C-level, with better communication between boards, CISOs and security teams[4].

Today's cybersecurity industry is influenced by three trends that have emerged in the past five years: (I) increasing digitisation of our commercial and private lives, our supply chains, cities, critical infrastructure and connected economy; (II) increasing sophistication, scale and visibility of attacks that target not only data, but our source of truth (sensors, ICS, news media); (III) emergence of international coalitions of companies, sharing threat intelligence and best-practices, challenged by national security agendas and data protection regulations.

We see the following developments that currently shape the cybersecurity environment: (I) an increasingly dynamic threat landscape; (II) new business models – among companies and criminal networks; (III) new technologies; (IV) stricter cybersecurity regulations; (V) a cyber dimension to every political conflict, mostly through highly active threat groups employing Advanced Persistent Threat (APT) tactics, often with nation-state backing and funding.





Dynamic and changing threat landscape
Cyberspace enables an ecosystem of support services (e.g. hackers for hire, Ransomware as a Service, bitcoin mining via botnet) that enhance the scale and reach of conventional crimes – at relatively low cost and lower risk compared to traditional crime. Criminals use the advantage of the global reach of the internet, crossing borders and jurisdictions, combined with anonymous and instant payments such as Bitcoin, to obfuscate their identity and build networks that can flexibly adapt to new opportunities.

Regulations
Companies are increasingly required to demonstrate good cybersecurity practice. Individual sectors such as maritime and finance are developing best practices and standardising their cybersecurity performance. Notable developments in 2017 included the US Cybersecurity Disclosure Act[5], which requires companies to justify any exclusion of cybersecurity expertise from their boards; and China's controversial national policy on cybersecurity[6], which became effective in June 2017, regulating how firms monitor and report security incidents. In Europe, the EU General Data Protection Regulation (EU GDPR) provides assurance for people in the EU and EEA on their personal data privacy and requires companies to ensure that same assurance for data used outside the EU. It also requires financial institutions to disclose any security breach within 72 hours of the breach incident. However, national policies are challenging for global companies to map and enforce within their infrastructure.

New business models
Organisations of all sizes and activities are increasingly relocating core business services to the cloud, using shared resources, with data as a service as a recognised business model. An increasingly mobile workforce is enabling new forms of operational structures, while traditional organizational boundaries are diminishing, evolving with increasing digitisation, remote working and hybrid workforces.

New technologies
Increased networking between fixed devices and IoT is enabling pervasive communication, blurring the lines between physical and virtual space. Artificial intelligence and data analytics are changing the way we interact and experience technology, across every facet of our private and commercial lives. Blockchain promises a new model of trust which enables entire new forms of business to emerge, especially in the financial sector[7], but has yet to be proven robust in enabling better cybersecurity.

Expanding Attack Surface

The human factors – communication, policies, innovation - should be considered in the context of a rapidly expanding global attack surface. In particular, it is expected that the **Internet of Things** (IoT) and the increase in the use of mobile devices will rapidly increase the number of internet-connected devices.

An estimated 8.4 billion networked devices and sensors will likely increase to 20.4 billion by 2020. With the rapid digitization of our private lives, public services and business supply chains, a single device – a smart car, a traffic sensor – represents an additional and very easy target: the threat of cyber hijacking in the new 'smart world' is now very real. Specialised search tools[8] reveal the IP address of vulnerable devices, including exposed Industrial Control Systems (ICS). Increasingly, routine business functions that rely on a sector of **critical infrastructure** – transport, communications, electricity, healthcare – are now vulnerable to attack through compromised ICS.

Until recently, power generation facilities and industrial plants have been 'air-gapped' from the internet, focusing security breach mitigation on preventing physical methods of intrusion, e.g. prohibiting the introduction of USB storage devices. In the interconnected age of IoT and fully integrated supply chains, the threat landscape is no longer limited to malware on USB sticks or malicious insiders. The Industrial Internet of Things (IIoT) is expected to add as much as $14.2 trillion to the global economy by 2023. Hardwired into the critical infrastructure of countries and regions, each of the sectors set to benefit from IoT will have a responsibility to mitigate the risks associated with interconnected services and supply chains.

With an ever-increasing array of devices and connected spaces, the IIoT and the 'bring your own device', **mobile workforce** redefines the traditional organisational perimeter that security teams are tasked to protect – and blurs the zone of cyber responsibility between companies, regulators and private households.

Trends in the Threat Landscape

The number and complexity of reported cybersecurity breaches has increased in 2018. Damage from even a single attack appears to be more extensive. The cascade effects of a single attack on a network or software that serves global supply chains are clear: for example, the WannaCry ransomware attack, which affected at least 100 countries, at an estimated cost of €6.5 billion.[9] Similarly, in 2017, the total cost of the NotPetya attacks which hit Maersk, a Europan-based logistics company, and other multinationals such as TNT Logistics is estimated have caused losses of at least €480 million.[10] The complexity of global supply chains connects data and devices across disparate networks of varying security quality, augmenting the global attack surface and increasing the number of possible entry-points for attackers seeking a gateway into companies, critical infrastructure and data services.

The complexity of global supply chains connects data and devices across disparate networks of varying security quality, augmenting the global attack surface

A comprehensive analysis of data breaches from November 2016 to October 2017 tallied 2,216 confirmed breaches worldwide[11]: the real total is likely much higher. The countries most negatively affected in 2017 included the US (at least 6.2 billion records), India (394 million records) and China (350.7 million).[12] In 2017, while Europe battled with ransomware, the US and Asia were prime targets for data breach and exfiltration[13]. Data breaches are now inevitable threat for any company that holds data which might have a value on the black market, or as blackmail leverage (for example, a ransom set against a GDPR fine of 4% of turnaround for non-compliance).

Attacks on governments, private sectors (finance, manufacturing) and state-owned entities continue[14], while thefts from organizations that rely entirely on the digital realm are now too frequent to occupy headline news for long: recent heists of data from Uber (December 2017)[15], cryptocurrency from Coincheck (January 2018)[16] and personal health records from the Government of Singapore (July 2018)[17] merge into a broader picture that suggests **the digital economy is fragile, vulnerable and inadequately protected**.

Major cybersecurity incidents of 2018 have so far featured (continued) data breaches, data exposures, attacks on devices at every scale from home routers to Industrial Control Systems and take-downs of local government systems: the City of Atlanta is still recovering from a ransomware attack in March that encrypted data at law firms and government services.[18] Continued heists on cryptocurrencies – at three times the thefts recorded for all of 2017 – have led to calls for crypto-currency anti-money laundering regulations.[19]

But threats to cybersecurity are not only about data theft and ransom. Attackers are no longer only interested in exfiltrating corporate data; they have expanded their focus to attempt control of infrastructure, coercion of entire communities and subversion of governance systems.[20] Attempted attacks on elections now appear inevitable: thefts of 9GB sensitive data during the French Presidential elections[21] (which the US attributed to Russia)[22] and the Dutch decision to use paper ballots and manual counting[23] are among many examples that suggest

> **the digital infrastructure of governmental functions and democracy is under attack.**

Ransomware is not new: the first case was seen in 2005, using methods proposed in 1996. But to really succeed as a business, ransomware needed three technologies: (i) strong, reversible encryption to lock and decrypt files; (ii) anonymous and confidential communication of keys and decryption tools; (iii) untraceable payments. The first to successfully demonstrate all three were CryptoLocker (2013) and CTB-Locker (July 2014). CTB is an acronym for Curve encryption, Tor browser and Bitcoin.

For cybercriminals, Bitcoin changed everything. With the formalisation of Bitcoin as a recognised exchange in 2012 (and others soon after), criminals found in cryptocurrencies everything they needed to rapidly build a financially-viable business model. Vastly simplifying the ransom payment process, Bitcoin was the paradigm shift that enabled a new threat, Ransomware as a Service (RaaS), to grow rapidly in 2016-17. Criminals lacking the technical skills to build and service their own ransomware can buy ready-made unlimited use packages, many of which include a payments processing system for as little as $40.

Cyber threats exist wherever human error, opportunity and ingenuity permit. The global attack surface is expanding rapidly (Internet of Things, prevalent smartphones, cloud services) and while the internet only reaches half the world's population, it is hardwired into the data services, critical infrastructure and financial systems that power most of the economy. Increasingly sophisticated threat actors, often operating from locations that lack the ability to enforce laws, currently enjoy a scale advantage and advantage of starting attacks from countries with little or no law enforcement: a successful attack must succeed only once, while cyber defence has to get it right all the time.

Predictions for 2018[24] identified a continuation in ransomware and election hacks, with an increase in the prevalence of ***ransomware as a service*** and hijacking of computers to mine cryptocurrencies. Cyber-physical attacks (targeting critical infrastructure) are now a reality, while the potential for using machine learning to create fake messages and media dis-information adds a new dimension to manipulating elections – and more. 2018 seemed to be the year where the effort to manipulate videos, known as 'deep fakes', became affordable to a wider range of people.

Ransomware as a Service 'product' comparison

Products	Price ($)	License	Share of ransom paid out to user (%)	Features
Hostman	49.95			Auto-decryption on ransom payout
Flux	45 / 150			
Satan	Free to download		70%	Users can set their own price and payment conditions
Atom			80%	
Stampado	39	Unlimited		Made by Rainmaker Labs, who later built Philadelphia. Payment options include Bitcoin, Paypal, bank transfer.
Philadelphia	389	Unlimited		Continually updated; Bitcoin payment autodetect
Frozr Locker	About 150			Encryption for 250 different filetypes
RaasBerry	C&C sub-scription 'packages' offered, from one month ($60) to three years ($650)		None	Ready-to-use ransomware that encrypts according to the parameters specified in sign-up. Provides 'testnet' mode so users can test in a virtual machine before distribution. Claims to avoid >90% of popular antivirus products.

(Source: Sophos; Barkly)

From the perspective of security professionals on the 'front line' of cyber defence, the five biggest problems in 2018 [25] are: (i) leaky clouds and badly mapped data assets; (ii) data heists that undermine core business and brand; (iii) keeping crypto-currency miners away from computer processing power; (iv) software developers and business strategists giving way to 'fast and simple' at the expense of security; and (v) preventing criminals from taking control of industrial control systems, particularly safety systems.

Research on the modus operandi and social networks of cybercriminals has evolved only in the past decade. A 2012 study found that nearly 80% of all cybercrime is perpetrated by organised criminal networks [26] which typically include at least three characters: (i) core members; (ii) enablers (e.g. providing scripting services); and (iii) money 'mules' (persons who illegally transfer acquired money on behalf of others).[27] Enablers often work for one or more networks, advertising their services through the Dark Net, while money mules number hundreds and are easily replaceable within the network. Challenging the stereotypes of the young lone hacker, nearly half the criminal network members identified in the European research were over the age of 35.

Six years later, new research presented at one of the industry's leading conferences finds that in cases analysed from twenty countries, organised criminal networks play a supporting role to a new breed of cybercriminal 'entrepreneurs', particularly in offline money laundering.[28]

Europe is a target but also as a significant source of cybercrime: in the first quarter of 2018, **38% of all cyber attacks worldwide originated from Europe.** Criminology research identifies three groups that have benefitted from the age of pervasive IT and internet: (1) traditional organised criminal groups, who use IT to augment the scale, reach and rate of their 'real-world' activities; (2) a new 'breed' of organised cybercriminal groups, who operate exclusively online, using the anonymity afforded by the Dark Net and virtual currencies; and (3) organised groups of ideologically and/or politically motivated people who use IT to achieve their objectives.[29]

Cybercriminal networks in Europe Cybercriminals rarely operate in isolation and may combine online and offline social networks to achieve their aim and adapt to the next opportunity. Methods and innovation among cyber criminals are evolving faster than law enforcement agencies and companies can adapt and attribution remains a vexing problem.[30] While the tactics and trust networks in organised crime remain largely unchanged in the new era of internet-augmented crime, today's cyber criminals enjoy a scale advantage, able to operate (and appear to operate) from any location via networks that exist on- and offline. Appearances may be deceptive: in March 2017 the UK National Crime Agency warned that cyber criminals are imitating nation state actors [31]; while in November 2017, the head of Europol reminded us [32] that cybercriminal gangs are organised, sophisticated and networked.[33] Cybercrime is big business.

38 %

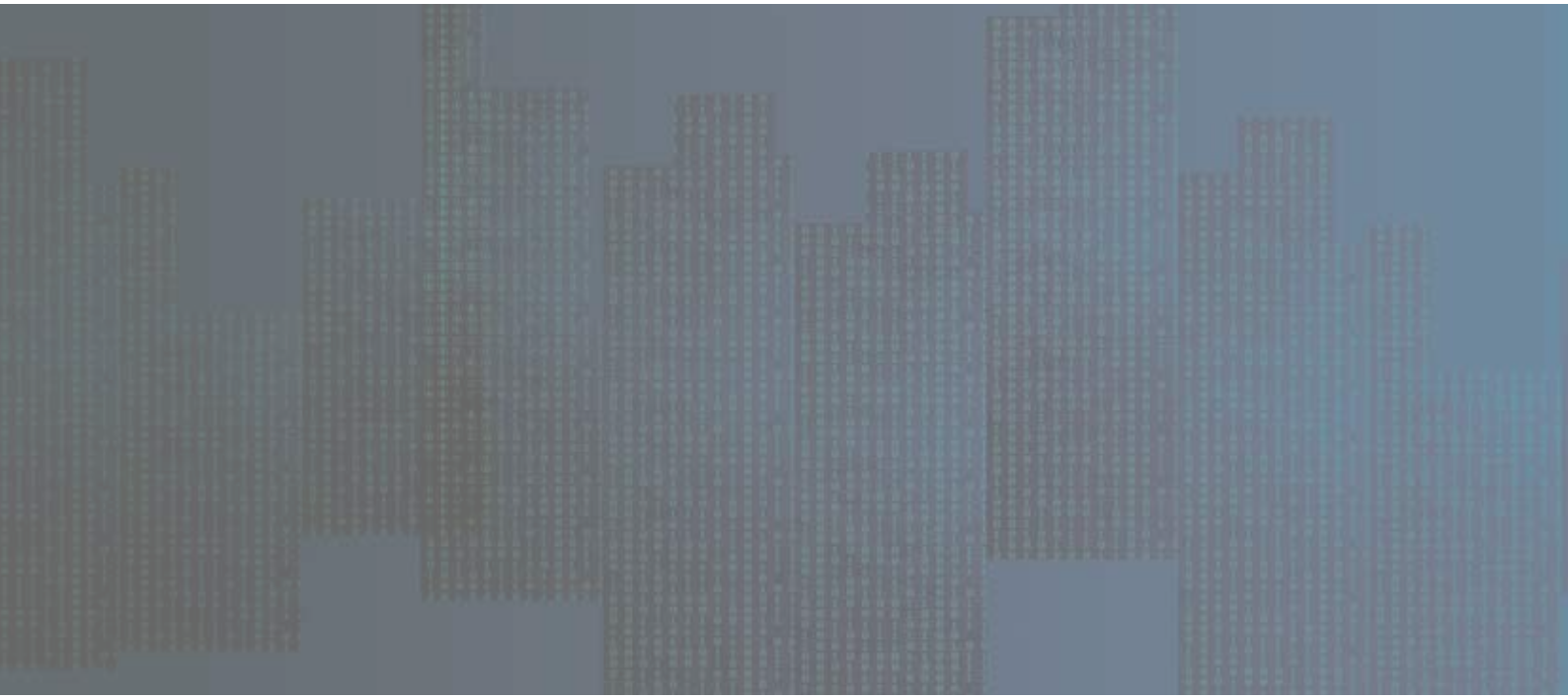
of all cyber attacks worldwide originated from Europe.

Source: Cosmos Direkt

Ransomware is not new but the methods have evolved. Cryptocurrencies are a gift to criminals: virtual currencies facilitate fast, global, secure and anonymous transactions. 2017 saw the rise of **Ransomware as a Service** (Raas), with 'kits' available on the Dark Net for as little as $40. In a similar category, Doxware attacks demand payment not for restoring access to files, but to prevent public disclosure of sensitive personal information.

Fileless malware is an uprising menace: using vulnerable services, attackers solely rely on putting their malicious code in the memory of the attacked system making it literally impossible for most antivirus to find them when searching the hard disk. In 2017, 42% of reported attacks were fileless malware, including attacks on 140 banks across 40 countries.

The original and simple goal of Distributed Denial of Service (DDoS) was to render a site or an intranet inoperable. Today, new criminal business models utilise DDoS as a service, with rates starting as low as $10 for an hour or $30 to $70 per day, via the Dark Net. New gigabit per second records are raising the bar of what attackers can accomplish: a record attack on the blog of security journalist Brian Krebs[34], with data rates of 660 Gbps in September 2016, was transcended in March 2018 when a central code sharing platform, Github, was hit by 1.7 Tbps .[35] Again not new, but enjoying a resurgence: increasingly sophisticated **phishing** attacks target one of the weakest links in cyber defence – the human factor.



A typology of threat actors

	Motivation	Resources	Attack styles
Lone or loosely coupled hackers	Glory, honour, fun, status	Script libraries, imagination, challenge (as hacker for hire)	Website defacements, fraud. Malware activation as hacker-for-hire. Ransomware.
Organized crime networks	Enhances existing capabilities, reduced costs of successful fraud / extortion attempt; low(er) cost methods for money laundering	Organised groups with strong trust relationships. Extended global reach through e.g. purchase of services via Dark Net.	Phishing (collecting access credentials), DDoS, Ransomware
Hacktivists	Political lobbying, campaigning on an issue deemed of ethical concern to citizens. Draw attention to a moral concern e.g. data privacy.	Organised groups, strict work sharing and trust relationships. Global reach.	Website defacements. Attacks on political parties. Targeted attacks on companies.
State-sponsored actor	Information warfare tasks (e.g. control narrative). Corporate espionage. Sabotage of (critical) infrastructure.	Financial resources. Cyber 'armies' who are loyal to their state / client.	Infrastructure sabotage (e.g. Stuxnet, Black Gold). Data theft, access to restricted information that has tactical advantage e.g. blueprints.

Effective Cyber Defence

Stealing digital currencies, subverting the outcome of elections, undermining companies and infrastructure. Over the past two years, attackers have shown [36] that it is not necessary to target every device or every person — just a few nodes or selected agents of change will suffice. Similarly, in cyber defence, organisational change starts with identifying group influencers, leaders and insider threats. Better insight into the criminal mindset and modus operandi (including social network analysis of underground forums) may help organisations to join in the effort required to break the cybercrime ecosystem.[37]

Cybersecurity is a battle in which the advantage goes to the organisation that can either attack or defend the most devices and networks. Contemporary cybersecurity has evolved from an era of prevention and perimeter defence, to a time of dynamic adaptation, where rapid detection and appropriate response is key for organisations who wish to survive the next attack.

Most companies today recognise that cybersecurity, in the first essential step, is fundamentally about identifying and managing risks.[38] The four questions executives typically ask are: (i) what is valuable within the organisation (assets); (ii) how / where do we need to protect our assets and interests; (iii) will it pay off to protect those assets?; and (iv) do we have enough qualified / skilled people to successfully defend these assets? At any scale – just as vulnerabilities arise from weaknesses in people, process and technology [39] – effective cybersecurity requires a blend of human and machine elements.

Trends in Defence Tools and Tactics

The most significant changes have been:

- a shift in focus from protecting the perimeter to additionally assuring the security of individual devices and data in transit, by considering end to end (E2E) security chains. This includes concepts like 'secure storage', hard disk encryption and encryption of communication channels using e.g. TLS – in which protection mechanisms follow the information architecture.
- a change in activity from system monitoring to proactive threat hunting, reactive security and behaviour analysis. Larger corporations have begun building 'red teams' for attacking their own assets and 'blue teams' for defending them. These teams co-exist with security operations teams tasked with running security appliances, however, organisational boundaries of knowledge-sharing and responsibility may not always be clear, adding another human dimension to the cybersecurity challenge;
- selective outsourcing of routine tasks such as security operations, security monitoring and threat intelligence feeds; and specialist one-off or recurring tasks such as forensic analyses, red-team tests and Dark Net investigations.

Core activities remain unchanged. For example, vulnerability management and patching remain vitally important tasks for security teams. 90% of attacks occur on unpatched systems; less than 1% are zero-day attacks. Most vulnerabilities are known and patches are available. The time taken between finding a vulnerability and deploying a patch takes far too long in many organisations: weeks, months or even years. Ideally, this should be less than 48 hours. Conversely, attackers are able to create exploits for published vulnerabilities within the unpatched days. Automation helps to reduce costs and increase efficiency, particularly across fragmented and disparate systems and teams.

Vulnerabilities in open and proprietary code are announced daily [40], security teams are processing tens or hundreds of millions of events, every day.[41] In the case of the open source Intrusion Detection System (IDS) Snort [42], the two most common alerts in 2017 were triggered by crypto-jacking malware. The rate and scale of security threats are too large for human teams to process without help. Automation is accelerating routine tasks such as security testing, penetration testing and code reviews.

Artificial Intelligence received great attention through 2017-18: while the principles and industry applications of AI within narrowly defined tasks are not new, AI is enjoying a new wave.[43] Within the field, machine learning is showing results. The DARPA 2016 Cyber Grand Challenge [44] showed that AI-powered cybersecurity is proven technology, creating self-healing computers.[45] Pioneers hope that AI can help fix vulnerable networks and deliver better cybersecurity, faster, augmenting the knowledge and reach of human security teams.

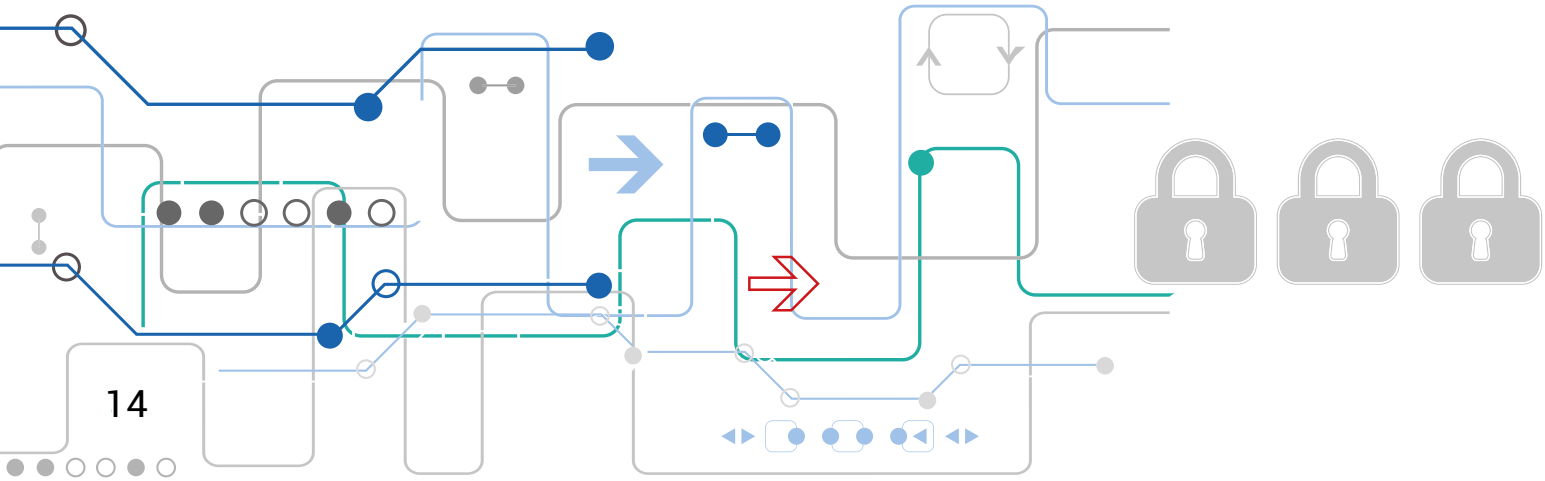
The New Defenders

Across Europe, the cybersecurity workforce includes diverse security professionals who perform an increasingly demanding range of tasks, including:

- Network security testing;
- Cyber threat hunting, collection, analysis and intelligence;
- Source code and malware analysis;
- Incident response;
- Digital forensics;
- Surveillance and network monitoring;
- Security audits, vulnerability analysis and penetration testing;
- Code and tool development and
- Insider threat investigation.

The core business of a cybersecurity team is protecting critical assets and denying advantage to the attacker. Security teams are typically focused on identifying and stopping attacks in real time, arresting the progress of malware across networks and devices, segmenting networks and continually patching machines on the networks they manage. Shared threat intelligence enables a more robust knowledge ecosystem. Cyber professionals collaborate, within their own team and across their industry, sharing insights and expertise via cybersecurity industry associations [46], several of which offer the industry-recognised certifications and continuous training [47] that hiring managers often seek. Beyond technical competencies, recruiters emphasise communication, social and analytical skills and rely heavily on their own social and professional networks to locate good candidates.[48] Practical skills, critical thinking and integrity are also sought-after traits in new recruits.[49]

Through 2016 -17, the cyber skills shortage was a headline theme at every major international event on cybersecurity. Worldwide, projections agree a shortfall of 1.8 million information security professionals by 2022.[50] Two thirds of information security professionals surveyed in 2017 reported they don't have enough staff to counter the threats their organisations face; estimates suggest Europe will have 350,000 more cybersecurity jobs than workers by 2022. Particularly in Europe and the US, a proliferation of upskilling and retraining programs aim to identify and train the missing skill sets. Companies are responding to the perceived shortage of talented security professionals by outsourcing, automating and investing in training. In Europe, many firms choose Managed Security Service Providers (MSSP) to boost their cybersecurity capabilities.



Next-generation Security Operations Centres (SOCs)

Even with help from machines, few organisations have the right skills, tools, data and knowledge in-house to build and retain a security team that can operate 24/7. Increasingly, companies in Europe are choosing to outsource their threat intelligence and security implementation requirements.

A SOC is "a team primarily composed of security analysts organized to detect, analyse, respond to, report on, and prevent cybersecurity incidents", providing services to a "bounded set of users, sites, IT assets, networks, and organizations".[51] The core function of the SOC – whether in-house or outsourced – is to collect and analyse data [52] from devices, networks and traffic the SOC is tasked to protect, identify and neutralise threats, limiting dwell time and lateral spread.

SOC design is unique to every organisation. No two organisations are exactly alike [53]; neither are their security cultures and requirements. Companies seeking to build or outsource a security operations team may benefit from an initial investment of time and effort to understand where, how and why data transactions occur across their workforce, supply chain partners, service providers and clients.

There are broadly four steps to consider in building the case for creating a SOC:

1. **Create an asset map.** This includes the people and knowledge already in house that will provide the contextual intelligence and points of contact – during the SOC design phase and incident response.
2. **Identify what to protect.** Include critical infrastructure, critical data and people that require continuous defence / monitoring. Threat modelling is useful here to identify the scenarios in which critical assets may be compromised.
3. **Identify the most valuable use-cases** and scenarios with the greatest impact on business continuity
4. **Create the blueprint**, deciding which parts to make / buy and identify how, where and when a SOC will complement or enhance core business strategy as part of the security strategy.

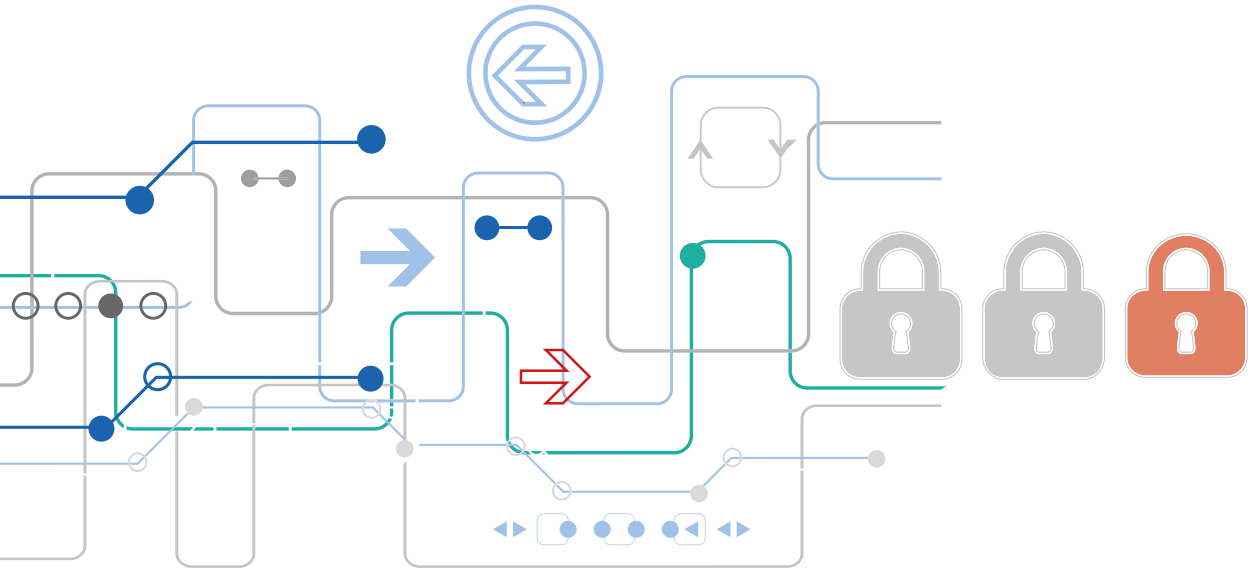
Considering outsourced SOC? Here are some questions to help guide your decision:

Can you recruit and retain the people you need?
Can you manage the organisational change that would come with implementing an in-house solution?
Can you fully manage external communications and brand management required during an incident response?
Can your security team operate on-demand, even around the clock?

SOCs run on data. The first step is to decide what types of data to collect, where and over what protocols. This might include network activity logs and telemetry data: in essence, taking the 'pulse' of the living data-driven organisation. SOC design should also consider timelag implications on the business system and networks. Using this baseline, static profile, the next phase is to optimise the data-collection capability [54] to the way the company works and calibrate all practices and tools so that they work together without disrupting 'business as usual' or imposing additional data management steps.

Next, consider how the data will be processed within the SOC: what parsing and normalization actions need to be done to create a usable source? Data analysis and security event correlation matches up incidents and potential problems with threat vectors that are of interest to the company. Identifying relationships between security events [55] often uses machine learning and anomaly detection. Comparing data against the known-good baseline helps to reveal unusual patterns.[56]

An effective SOC is not just for threat monitoring and reporting, it's a core part of the intelligence fusion centre for any organisation that wants to survive in the cyber era. Every organisation's business intelligence, audit and knowledge management functions rely on a secure data infrastructure. In this sense, the SOC can be viewed as the core requirement for survival in the digital economy.



A Perspective from Detecon's Cybersecurity Experts

Cyber attacks are a real challenge for companies of every size and activity, today more than ever before. The vulnerabilities created by an internet-enabled world, augmented by an increasingly pervasive IoT and the availability of nearly anonymous currencies, are currently limited only by the imagination of those who seek to profit. For many companies across Europe, organised crime and lone actors currently enjoy a scale advantage, which may only increase in future as criminals exploit vulnerabilities in our social fabric.

Risks are augmented by four features of the modern business environment:

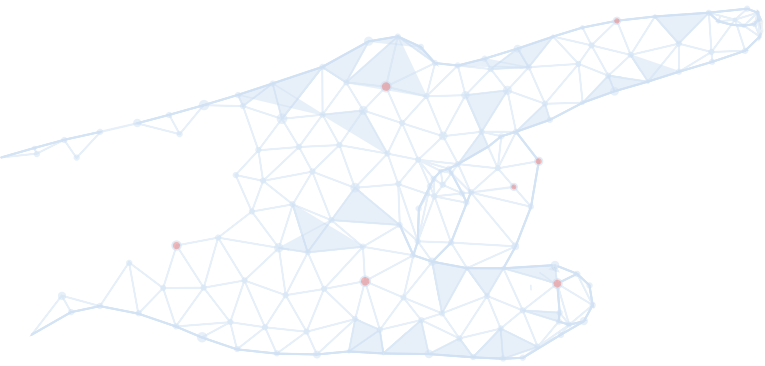
- Transient, location-independent workforce
- Corporate knowledge that's physical (held by people) and virtual (metadata and deep web)
- Merging of cyber and physical structures
- An expanding attack surface that's no longer contained within the organisation

Cybersecurity is the cost of doing business in the digital age and essential for almost every company in order to protect the business from interruptions, misuse of data or blackmailing. A good cybersecurity foundation comprises of:

- Getting the basics right (patching, asset control, skills);
- Choosing a risk-based approach, identifying what assets require protection, defining how and where effort will optimise cybersecurity performance;
- Continual education, understanding how to navigate changes in regulatory environments and anticipate where and how new technology requires new learning within the firm.

Organisations that want to thrive in the digital future must urgently assess the vulnerabilities and most valued assets in their internal knowledge, practice and data. Many may want to consider building a SOC that works for how they want to do business.

There is no single technology or service that can combat cyber attacks, as it encompasses much more than IT. No team, however proficient in the language and social skills needed for advanced threat intelligence, can provide total security. Cybersecurity is an organisational challenge, requiring changes in how we do business, with the familiar combination of process, technology and people skills.



Authors

Matthias Gruber is a Cybersecurity expert and leads the Detecon Cybersecurity team. He consults clients on their cyber defence strategies, SOC evaluation as well as implementation and reviews of their current cybersecurity posture.

https://www.linkedin.com/in/matthiasgruber/

@matgrube

Andrea Tribelhorn is a Managing Consultant at Detecon with more than 8 years of experience in the field of Cyber-security. She consults clients from various industries. Her area of expertise includes cyber defence strategies as well as Cybersecurity governance, concepts, frameworks, guide-lines and processes.

https://www.linkedin.com/in/andrea-tribelhorn/

Dr. Aubrey-Derrick Schmidt is a technical Cybersecurity Consulting Expert working at Detecon Digital Engineering Center in Berlin. At Detecon Digital Engineering Center, he works with several customers on protecting new and innovative solutions in various fields, following new approaches in addressing security problems in given fields.

https://www.linkedin.com/in/aubreyschmidt/

Company Profile

Management consulting with pronounced technology expertise

Detecon International is a globally active management consultancy that combines classic management consulting and pronounced technology expertise. After all, considering both at the same time determines the future performance of every company.

Digital technologies and networks

Our business is consulting, our strength digital technologies and networks. For 40 years, we have been helping companies and telecommunications providers around the world to sustainably improve their competitiveness and performance across the entire value chain with the help of innovative technologies. We also offer our clients solutions in all areas of classic management consulting: digital business models, organization, processes and HR management.

Bridge between business and ICT

We build the bridge between business and ICT perspectives. With this ability, we guide our customers through the digital transformation. Detecon is a subsidiary of T-Systems International, the corporate customer brand of Deutsche Telekom.

Footnotes

1. Defence companies target the cyber-security market', Economist, 26 July 2018 [https://www.economist.com/business/2018/07/26/defence-companies-target-the-cyber-security-market]
2. Data from a survey of 3,000 individuals in a cross-section of industries.Hiscox Cyber Readiness Report 2017, Hiscox Global [http://www.hiscox.com/cyber-readiness-report.pdf]
3. CSIS (2018), 'Economic Impact of Cybercrime', 21 February 2018 [https://www.csis.org/analysis/economic-impact-cybercrime]
4. The Evolving Role of CISOs', Ponemon Institute LLC, August 2017.
5. The US Cybersecurity Disclosure Act [https://www.congress.gov/115/bills/s536/BILLS-115s536is.pdf]
6. China adopts cybersecurity law in face of overseas opposition', Reuters, 7 November 2016 [http://www.reuters.com/article/us-china-parliament-cyber-idUSKBN132049]
7. The EU General Data Protection Regulation [http://www.eugdpr.org/]
8. Shodan [https://www.shodan.io/explore/category/industrial-control-systems]
9. Global cyber attack could spur $53 billion in losses: Lloyd's of London', Reuters, 17 July 2017 [https://www.reuters.com/article/us-cyber-lloyds-report/global-cyber-attack-could-spur-53-billion-in-losses-lloyds-of-london-idUSKBN1A20AB]
10. Not Petya's fiscal impact: $592.5 million and growing', Cybereason, 6 September 2017 [https://www.cybereason.com/blog/blog-notpetyas-fiscal-impact-592-5-million-and-growing]
11. 2018 Data Breach Investigations Report', Verizon [https://www.verizonenterprise.com/verizon-insights-lab/dbir/]
12. Gemalto Data Breach Index [https://www.breachlevelindex.com/]. Note: data includes publicly disclosed breaches only – it is likely the true number of breaches is much higher.
13. ISC² 2017 Global Information Security Workforce Study (EMEA) [https://www.isc2.org/-/media/Files/Research/GISWS-Report-Europe.ashx]
14. Significant cyber incidents', Center for Strategic and International Studies, 2018 [https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity]
15. in December 2017, data for 57 million drivers and an undisclosed number of customers was stolen from Uber AWS, with Uber liable for around $100,000 of damages
16. 'The Coincheck hack and the issue with crypto assets on centralized exchanges', Reuters, 29 January 2018 [https://uk.reuters.com/article/us-japan-cryptocurrency-q-a/the-coincheck-hack-and-the-issue-with-crypto-assets-on-centralized-exchanges-idUKKBN1FI0K4]
17. 'Personal info of 1.5m SingHealth patients, including PM Lee, Stolen in Singapore's worst cyber attack', Straits Times, 20 July 2018 [https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most]
18. Atlanta officials reveal worsening effects of cyber attack', Reuters, 6 June 2018 [https://www.reuters.com/article/us-usa-cyber-atlanta-budget/atlanta-officials-reveal-worsening-effects-of-cyber-attack-idUSKCN1J231M]
19. 'Cryptocurrency exchange theft surges in first half of 2018: report', Reuters, 3 July 2018 [https://www.reuters.com/article/us-crypto-currencies-ciphertrace/cryptocurrency-exchange-theft-surges-in-first-half-of-2018-report-idUSKBN1JT1Q5
20. J. Burton, 'The US election hack, fake news, data theft: the cybersecurity lessons from 2017', The Convseration, 25 December 2017 [https://theconversation.com/the-us-election-hack-fake-news-data-theft-the-cyber-security-lessons-from-2017-89280]
21. 'Hackers hit Macron with huge email leak ahead of French election', Wired, 5 May 2017 [https://www.wired.com/2017/05/macron-email-hack-french-election/]
22. The NSA confirms it: Russia hacked French election 'infrastructure", Wired, 9 May 2017 [https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/]
23. Dutch will hand count ballots due to hacking fears', Reuters. 1 February 2017 [https://www.reuters.com/article/us-netherlan ds-election-cyber/dutch-to-hand-count-ballots-due-to-hacking-fears-rlt-idUSKBN15G55A]
24. Martin Giles, 'Six Cyber Threats to Really Worry About in 2018', MIT Technology Review, 2 January 2018 [https://www.technologyreview.com/s/609641/six-cyber-threats-to-really-worry-about-in-2018/]
25. 'The five most dangerous new attack techniques', SANS Institute, RSA 2018 Keynote [https://www.sans.org/the-five-most-dangerous-new-attack-techniques]

26. BAE Systems research reveals the real perpetrators of digital crime', BAE Systems, 28 March 2012 [https://www.baesystems.com/en/article/bae-systems-research-reveals-the-real-perpetrators-of-digital-crime]
27. 'Dutch will hand count ballots due to hacking fears', Reuters. 1 February 2017 [https://www.reuters.com/article/us-netherlan ds-election-cyber/dutch-to-hand-count-ballots-due-to-hacking-fears-rlt-idUSKBN15G55A]
28. K. Jackson Higgins, 'No, the Mafia Doesn't Own Cybercrime: Study', Dark Reading, 8 August 2018 [https://www.darkreading.com/threat-intelligence/no-the-mafia-doesnt-own-cybercrime-study/d/d-id/1332488]
29. The NSA confirms it: Russia hacked French election 'infrastructure", Wired, 9 May 2017 [https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/]
30. T. Rid and B. Buchanan, 'Attributing Cyber Attacks', The Journal of Strategic Studies, 38:1-2, pp.4-37. DOI: 10.1080/01402390.2014.977382
31. 'New assessment warns industry that cyber criminals are imitating nation state attacks', NCA, 14 March 2017 [http://www.nationalcrimeagency.gov.uk/news/1043-new-assessment-warns-industry-that-cyber-criminals-are-imitating-nation-state-attacks]
32. https://twitter.com/rwainwright67/status/928338389128155136
33. 'Fast-growing cyber crime threatens financial sector: Europol', Reuters, 8 November 2017 [https://www.reuters.com/article/us-portugal-websummit-europol/fast-growing-cyber-crime-threatens-financial-sector-europol-idUSKBN1D82QS
34. Krebs on Security [https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/]
35. ZD Net [https://www.zdnet.com/article/new-world-record-ddos-attack-hits-1-7 tbps-days-after-landmark-github-outage/]
36. J. Koetsier, 'How To Hack An Election: $50, 60 Minutes, And Fake Ads On Facebook', Forbes, [https://www.forbes.com/sites/johnkoetsier/2017/10/11/how-to-hack-an-election-50-60-minutes-and-fake-ads-on-facebook/#62a3d3d05760]
37. Cambridge Cybercrime Centre: Third Annual Cybercrime Conference, 12 July 2018 [https://www.cambridgecybercrime.uk/conference2018.html]
38. Cybersecurity: the cost of immaturity', The Economist, 12 November 2015
39. – 40: J. Muniz, G. McIntyre and N. AlFardan (2016), 'Security Operations Center: Building, Operating and Maintaining Your SOC'. (Cisco Systems Inc.: Indianapolis)
41. C. Zimmerman (2014), 'Ten Strategies of a World-Class Cybersecurity Operations Center'. (The MITRE Corporation: Bedford, MA; McLean, VA)
42. [https://twitter.com/snort/status/1030209825668509701?s=03]
43. Corea, F. Artificial intelligence and exponential technologies: business models evolution and new investment opportunities. (Springer, 2017).
44. 2016 Cyber Grand Challenge, DARPA [http://archive.darpa.mil/cybergrandchallenge/index.htm]
45. A. O. Hall (2017), 'Investing in Cybersecurity Solutions', Cyber Defence Review, 2, 9–12.
46. 'Cybersecurity Industry Associations', Cyberventures, 2018 [https://cybersecurityventures.com/cybersecurity-associations/]
47. see for example [https://cybersecurity.isaca.org/csx-nexus]
48. ISC² 2017 Global Information Security Workforce Study [https://www.isc2.org]
49. G.V. Hulme, 'Six entry-level cybersecurity job seeker failings', CSO, 10 March 2015 [https://www.csoonline.com/article/2894193/it-jobs/six-entry-level-cybersecurity-job-seeker-failings.html]
50. see e.g. RSA Conference 2018
51. C. Zimmerman (2014), 'Ten Strategies of a World-Class Cybersecurity Operations Center'. (The MITRE Corporation: Bedford, MA; McLean, VA).
52. J. Muniz, G. McIntyre and N. AlFardan (2016), 'Security Operations Center: Building, Operating and Maintaining Your SOC'. (Cisco Systems Inc.: Indianapolis). H. Mintzberg, "Species of Organizations," Apr. 14, 2016, http://www.mintzberg.org/blog/organization-species
53. – 56: J. Muniz, G. McIntyre and N. AlFardan (2016), 'Security Operations Center: Building, Operating and Maintaining Your SOC'. (Cisco Systems Inc.: Indianapolis)

Published by
Detecon International GmbH.
www.detecon.com

www.detecon.com
cybersecurity@detecon.com

Abu Dhabi • Ankara • Bangkok • Berlin • Bratislava • Budapest • Dresden • Dubai • Frankfurt/Main • Istanbul
Johannesburg • Cologne (HQ) • Moscow • Munich • Beijing • San Francisco • Warsaw • Vienna • Zurich

DETECON
CONSULTING