FORESIGHT 2030 THREATS

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY
20 years!

MARCH 2024

EXECUTIVE DIRECTOR FOREWORD

In today's world, the growing reliance on digital technologies, such as AI, across all sectors has introduced both opportunities and threats in the cybersecurity ecosystem. Amidst worldwide geopolitics and natural disasters, cyberattacks have become more sophisticated and hybrid threats have gained prominence.

We are currently faced with a rapidly changing cyber threat landscape. To successfully address what the future might bring, we have to continuously adapt our posture, tools and strategies.

The EU Agency for Cybersecurity remains committed to its mission to increase the common level of cybersecurity across the EU, by building resilience against the emerging cybersecurity risks and threats. In order to be able to remodel our approach and shield our critical infrastructure, we need to be vigilant to the upcoming cybersecurity trends.

The second edition of the Foresight Cybersecurity Threats for 2030 is a result of the applied foresight methodology along with the valuable contributions from cybersecurity experts. This booklet provides a comprehensive overview of the top emerging cybersecurity threats and identified trends that lie ahead and eventually aims to improve preparedness and enable better informed actions

Juhan Lepassaar
Executive Director

Reference to the report page:
https://www.enisa.europa.eu/new-foresight-2030

SUPPLY CHAIN COMPROMISE OF SOFTWARE DEPENDENCIES

1

WHAT IF...

State-sponsored actors insert a backdoor in a well-known and popular open-source library on online code repository. They use this to infiltrate information from most major European corporations and use the information to blackmail leaders, espionage, or otherwise initiate disruptions across the EU.

More integrated components and services from third party suppliers and partners could lead to novel and unforeseen vulnerabilities with compromises on the supplier and customer side.

POTENTIAL THREAT ACTORS

State-sponsored groups, criminal organisations

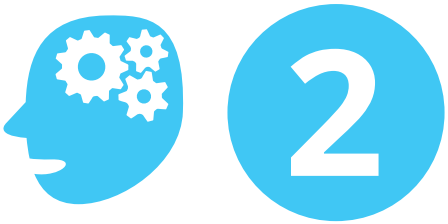
POTENTIAL METHODS

Sabotage, theft, network reconnaissance, malicious code, abuse of information leakage

POTENTIAL IMPACTS

Disruption, malfunction, data loss, data leakage

SKILL SHORTAGES



WHAT IF...

The skill shortage leads to an increase of online job advertisements that tell attackers the technologies that each organisation is using and the approximate number of empty positions. A state-sponsored actor may use this to their advantage as a part of a larger campaign to tamper with critical infrastructure in another country.

Lack of capacities and competencies could see cybercriminal groups target organisations with the largest skills gap and the least maturity.

POTENTIAL THREAT ACTORS

Cybercrime actors, hackers-for-hire, state-sponsored actors

POTENTIAL METHODS

Spear phishing attacks, social engineering

POTENTIAL IMPACTS

Financial damage, outages

HUMAN ERROR AND EXPLOITED LEGACY SYSTEMS WITHIN CYBER-PHYSICAL ECOSYSTEMS

WHAT IF...

Manuals for all legacy OT equipment are available online and studied primarily by state-sponsored groups. Once a vulnerability is found, they target user devices or other IoT products used at the plant. Cyber criminals begin a new form of ransomware in which they bring down important infrastructure and demand payment, given that the operator likely lacks the resources to solve the issue themselves.

The fast adoption of IoT, the need to retrofit legacy systems and the ongoing skill shortage could lead to a lack of knowledge, training and understanding of the cyber-physical ecosystem, which can lead to security issues.

POTENTIAL THREAT ACTORS

State-sponsored groups, cyber criminals, hacktivists

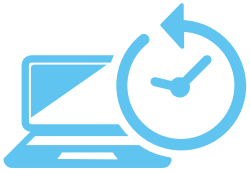
POTENTIAL METHODS

Tampering, failure of communication links, denial of service, malicious activity, manipulation of information, targeted attacks, brute force, unauthorised physical access

POTENTIAL IMPACTS

Malfunction, failures and outages, physical damage

EXPLOITATION OF UNPATCHED AND OUT-OF-DATE SYSTEMS



4

WHAT IF...

Criminals exploit a vulnerability in an unpatched component of critical infrastructure owned by a private company currently going bankrupt which cannot afford the few subject matter experts or the support contract that can respond to the attack. On the other side attackers launch a ransomware attack towards out of date hospital systems that cannot be patched because the manufacturer doesn't provide updates anymore.

Everything-as-a-service leads to a multitude of tools and services that require frequent and synchronised updates as well as orchestrated maintenance. This fact along with the skill shortage, results in an extended and unmanageable surface of vulnerabilities that threat actors can exploit.

POTENTIAL THREAT ACTORS

State-sponsored groups, criminal organisations, hacktivists

POTENTIAL METHODS

Tampering, failure of communication links, denial of service, malicious activity, manipulation of information, targeted attacks, brute force, malicious code

POTENTIAL IMPACTS

Malfunction, failures and outages, physical damage, damage/loss, unavailable critical infrastructure

RISE OF DIGITAL SURVEILLANCE AUTHORITARIANISM / LOSS OF PRIVACY

5

WHAT IF...

An authoritarian regime uses their power to retrieve databases of information about individuals who have visited their country, from both public and private entities. They track all those who participated in anti-government protests, put them on a watch list, and subsequently are able to manipulate those individuals' access to national services like voting, visits to their healthcare providers, or access to other online services.

Facial recognition, digital surveillance on internet platforms or digital identities data stores may become a target for criminal groups.

POTENTIAL THREAT ACTORS

State-sponsored groups, criminal organisations

POTENTIAL METHODS

Man in the middle, malicious software, use of rogue certificates, abuse of personal data

POTENTIAL IMPACTS

Privacy breaches, human rights abuses

CROSS-BORDER ICT SERVICE PROVIDERS AS A SINGLE POINT OF FAILURE

6

WHAT IF...

A state-sponsored actor aims to temporarily cripple a region during an active conflict by installing malware that disrupts all critical functions of the ICT provider. Without operational cities, roadways, and communication channels, the region is essentially crippled without the ability for civilians to go about their daily lives and the responsible parties limited in their ability to maintain defense monitoring systems and to collaborate to develop response options and methods for bringing the necessary systems back online.

ICT sector connecting critical services such as transport, electric grids and industry that provide services across borders are likely be to targeted by techniques such as backdoors, physical manipulation, and denials of service and weaponised during a future potential conflict.

POTENTIAL THREAT ACTORS

State-sponsored actors, hackers-for-hire

POTENTIAL METHODS

Fraud, theft, corruption, terrorist attack, network traffic manipulation, manipulation of hardware or software, abuse of authorisations

POTENTIAL IMPACTS

Outages, damage/loss, unavailable critical infrastructure

ADVANCED DISINFORMATION CAMPAIGNS

7

WHAT IF...

A state-sponsored actor may impersonate a political rival by using deepfakes and spoofing the candidate's digital identity, significantly impacting election results.

Deepfake attacks can manipulate communities for (geo) political reasons and for monetary gain.

POTENTIAL THREAT ACTORS

State-sponsored groups, criminal organisations, hacktivists

POTENTIAL METHODS

Fraud, unauthorised access, session hijacking, identity theft, abuse of personal data

POTENTIAL IMPACTS

Distrust, disinformation, financial damage, foreign information manipulation and interference (FIMI)

RISE OF ADVANCED HYBRID THREATS

8

WHAT IF...

Hackers are hired by a corporation to investigate the new technology being developed by a competitor. In their quest, they are able to retrieve metadata, view code, and set up a machine learning algorithm that continuously collects changes to the code and then continuously accesses user account to prevent monitoring systems from recognising that the attacker is in the network. In parallel they obfuscate the activity by spreading fake news about insider trading and industrial espionage from a third competitor by dropping fake evidence of physical intrusion.

Physical or offline attacks are evolving and becoming often combined with cyberattacks due to the increase of smart devices, cloud usage, online identities and social platforms.

POTENTIAL THREAT ACTORS

State-sponsored actors, hackers-for-hire, cyber criminals

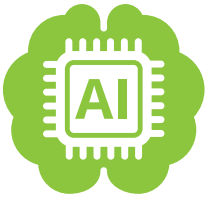
POTENTIAL METHODS

Unauthorised access, social engineering, abuse of personal data, remote command execution, malicious activity

POTENTIAL IMPACTS

Privacy breaches, outages, failures/malfunctions

ARTIFICIAL INTELLIGENCE ABUSE



WHAT IF...

A state-sponsored actor wants to sow discord in a population before an election and manipulates the learning data of a law enforcement algorithm to target specific populations, causing widespread protests and violence. They are also able to deduct information about the political opponents themselves by using an AI analysis of the individuals' whereabouts, health history, and voting history – the correlation of such personal data will likely only be feasible with the use of AI tools.

Manipulation of AI algorithms and training data can be used to enhance nefarious activities such as the creation of disinformation and fake content, bias exploitation, collecting biometrics and other sensitive data, military robots and data poisoning.

POTENTIAL THREAT ACTORS

State-sponsored actors, cyber criminals, hackers-for-hire

POTENTIAL METHODS

Spoofing, denial of service, malicious code, unauthorised access, targeted attacks, misuse of information, man in the middle attack

POTENTIAL IMPACTS

Biased decision-making, privacy violations, foreign information manipulation and interference (FIMI)

PHYSICAL IMPACT OF NATURAL/ ENVIRONMENTAL DISRUPTIONS ON CRITICAL DIGITAL INFRASTRUCTURE

10

WHAT IF...

The increasingly common occurrences of fires and flooding result in more frequent power outages, leading to disruptions in connectivity services. Techno luddites weaponise this and perform physical attacks to back up sites.

The increased severity and frequency of environmental disasters following climate change may cause several unforeseen regional outages. Redundant back-up sites that maintain the availability of critical infrastructure are also impacted by the massive and extreme weather phenomena

POTENTIAL THREAT ACTORS

State-sponsored actors, hacktivists

POTENTIAL METHODS

Tampering, terrorist attack, sabotage, theft, manipulation of hardware

POTENTIAL IMPACTS

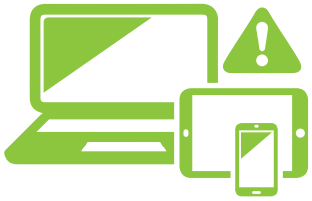
Outages, damage/loss, unavailable critical infrastructure, disruption, malfunction, data loss

2030 TOP THREATS CONTINUED

11

LACK OF ANALYSIS AND CONTROL OF SPACE-BASED INFRASTRUCTURE AND OBJECTS

State-sponsored attackers access space infrastructure, build up their capabilities and knowledge of the technology, and secure their presence to execute attacks. Their aim may be to create infrastructure malfunctions as a statecraft tool to sabotage other governments or commercial space operations and systems during geopolitical conflicts. Due to the intersections between private and public infrastructure in space, the security of these new infrastructures and technologies need to be investigated as a lack of understanding, analysis and control of space-based infrastructure can make it vulnerable to attacks and outages.



12

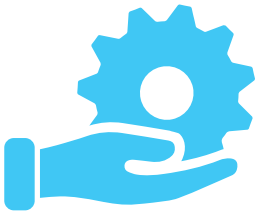
TARGETED ATTACKS (E.G. RANSOMWARE) ENHANCED BY SMART DEVICE DATA

Cybercriminals may use the increased amount of available data from smart devices and analyse it with AI to create behavioral models of their victims for spear phishing campaigns or stalking. Through data obtained from internet-connected smart devices, attackers can access information for tailored and more sophisticated attacks.

13

INCREASED DIGITAL CURRENCY-ENABLED CYBERCRIME

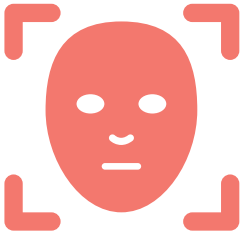
By 2030, digital currency-enabled cybercrime will increase rapidly. Cryptocurrencies, and the broad market adoption of them, already have enabled organised crime to expand their reach. Because digital currencies will be very commonly used as an investment asset and means of payment in European markets, organised crime may be able to expand their targets. This means that cybercrime groups offering professional services (cyber-attacks) will be better funded because of an increase in the efficiency and effectiveness of their efforts.



14

MANIPULATION OF SYSTEMS NECESSARY FOR EMERGENCY RESPONSE

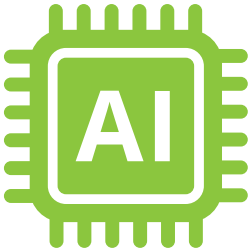
Manipulation of sensors with connections to emergency services may overload services like ambulances, police, firefighters, etc. For example, call centres may be overloaded with inauthentic calls or fire alarms may be manipulated to injure specific individuals or to obscure emergency response teams' ability to locate the issue. Similarly, mass panics that overload emergency systems may also be provoked through the use of social media.



15

TAMPERING WITH DEEPFAKE VERIFICATION SOFTWARE SUPPLY CHAIN

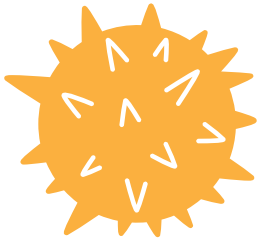
By 2030, deepfake technology will be widely used. It may be used as a form of harassment, evidence tampering, and provoking social unrest. Although there will likely be a rapid influx of verification software that analyses videos and voice to verify the identity of individuals , the urgent market demand leads to programmers cutting corners. This software will be highly targeted by anyone wishing to use deepfakes for illegal or unethical purposes.



16

AI DISRUPTING / ENHANCING CYBER ATTACKS

Escalation as a result of AI-based tools. Attackers will use AI-based technologies to launch attacks. In order to defend against those attacks and even to launch counter measures, there must also be defensive AI-based weapons. Behaviour of the AI in these cases is difficult to test, measure and control – if speed of response is valued.



17

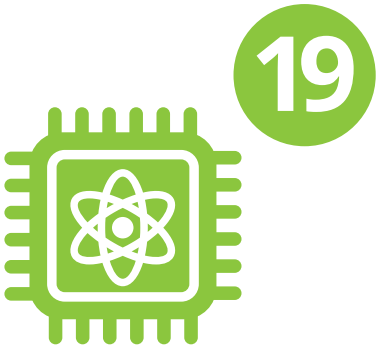
MALWARE INSERTION TO DISRUPT FOOD PRODUCTION SUPPLY CHAINE

Due to increased automatisation and digitalization of food production, food supply chains can be disrupted by a range of threat actors with medium-high resources. Denial of service attacks on packaging plants, for example, can prevent continued food operations; processed food manufacturing tools may be manipulated to change the compounds in the food itself. Attacks like these can lead to a food shortage, economic disruptions, and in the worst case, poisoning.

18

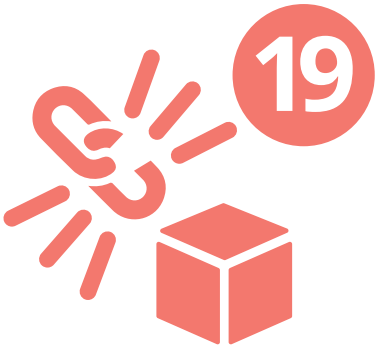
EXPLOITATION OF E-HEALTH (AND GENETIC) DATA

The amount of genetic and health data increases tremendously by 2030 and is in the hands of many stakeholders in the public and private sectors. Vulnerabilities in e-health devices and databases containing very sensitive and/or genetic information may be exploited or used by criminals to target individuals or by governments to control populations, e.g., using diseases and genetic diversity as a reason for discriminating against individuals. Genetic data may further be abused to aid law enforcement activities like predictive policing or to support a more regimented social credit system.



ATTACKS USING QUANTUM COMPUTING

In 2030 quantum computing resources will be made more widely available, allowing threat actors to use quantum computing to attack existing deployments of public key cryptography. Likewise, there is a risk that threat actors collect sensitive encrypted data now, aiming to decrypt it once quantum computing is accessible. This is especially relevant for current digital IDs that use asymmetric cryptography to authenticate.



DISRUPTIONS IN PUBLIC BLOCKCHAINS

Blockchain has been implemented in nearly all aspects of society in 2030. Unfortunately, security expertise in the area of blockchain did not advance significantly, creating a slew of vulnerabilities that may be exploited in the future. Locally unavailable blockchain technology will, for example, prevent access to voting, legal transactions, and even security systems. Another possible attack vector is exploited by partitioning the bitcoin network by hijacking IP address prefixes. This can cause, for example, duplicated spending and thus economic damage.

TECHNOLOGICAL INCOMPATIBILITY OF BLOCKCHAIN TECHNOLOGIES

Until 2030, several regionally based blockchain technologies are created by different groups of governments to create an international "gold standard". This is driven by a societal lack of trust in blockchain that has accumulated over the last years. Each technology group aims to gain a competitive advantage. This gives rise to a period of technological incompatibility of blockchain technology which leads to failures, malfunctions, data loss and the exploitation of vulnerabilities at the interfaces of the different blockchains. This creates challenges for ecosystem management and data protection, furthers distrust, and negatively affects trade and GDP growth.

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

https://www.enisa.europa.eu/topics/foresight