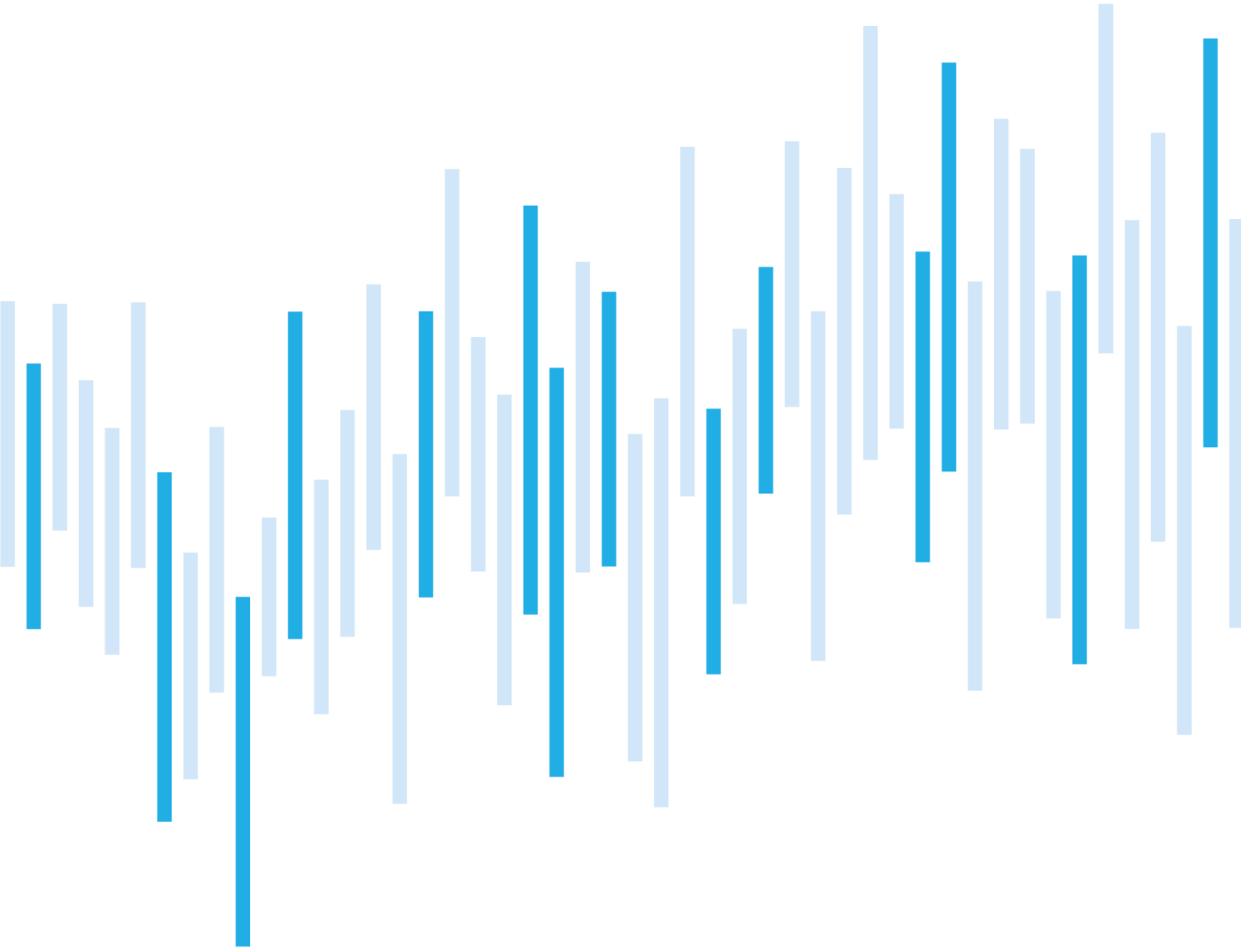
CYBER SECURITY INCIDENTS FROM NÚKIB'S PERSPECTIVE

APRIL 2025



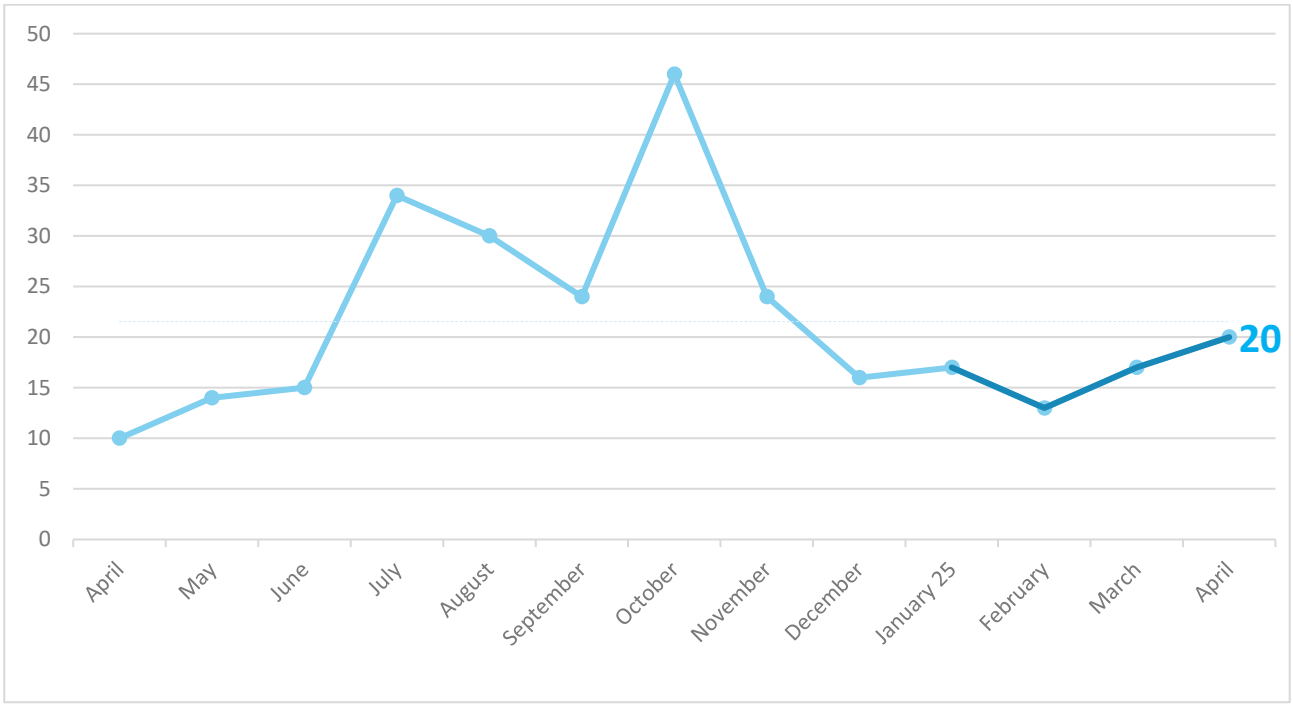
National Cyber and Information Security Agency

Summary of the Month

During April, NÚKIB recorded 20 cyber security incidents, continuing the gradual rise to average values. The most prevalent category was Availability (6 incidents), most of which involved service outages. The Information Security category (5) consisted exclusively of ransomware attacks reflecting the ongoing trend of increased ransomware activity that NÚKIB has been recording – with exceptions – since September of last year. The Intrusion category (3) consisted primarily of phishing, while Attempted Intrusion (2) involved vulnerabilities in Ivanti VPN software. The Malicious Code category (2) included, for example, the spread of spam via malware. The Fraud (1) involved a successful spear-phishing attack that resulted in financial loss.

In terms of severity, two incidents related to Ivanti VPN vulnerabilities were classified as significant. The remaining 18 were considered less significant. NÚKIB recorded 8 cyber events in April, including infrastructure scanning, fraudulent websites, extortion and vishing (fraudulent phone calls).

Number of cyber security incidents reported to NÚKIB



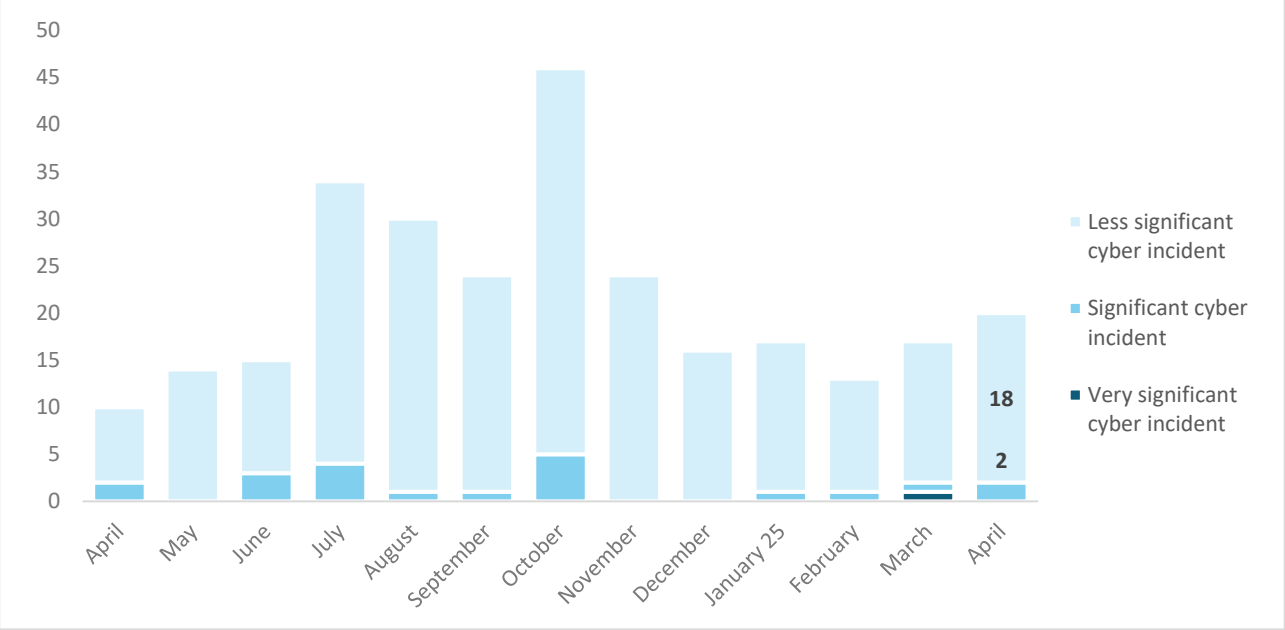
This report provides a summary of the month's events. The data, information and conclusions presented herein are primarily based on cyber incidents reported to NÚKIB. Where information from open sources is used, the source is always clearly indicated.

Please note that some values in the incident log may be subject to retrospective updates. As a result, historical data presented in graphs may change over time.

Comments and suggestions for improving the report can be sent to komunikace@nukib.cz

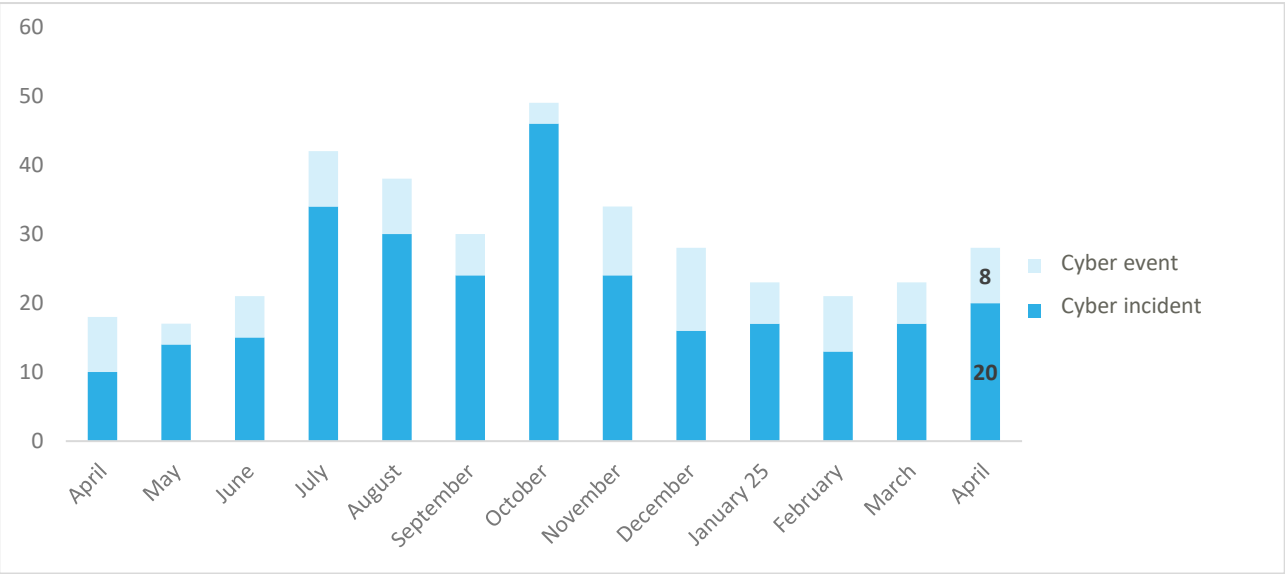
Severity of the Handled Cyber Security Incidents

NÚKIB determines the severity of cyber incidents on the basis of Decree No. 82/2018 Coll. and its internal methodology.



Ratio of Recorded Cybersecurity Incidents to Cybersecurity Events[1]

As part of its activities, NÚKIB receives, processes and evaluates reports related to cybersecurity. Based on the analysis, each report is classified as either a cybersecurity incident, a cybersecurity event or a non-relevant submission. The graph below illustrates the ratio between recorded cybersecurity incidents and cybersecurity events.



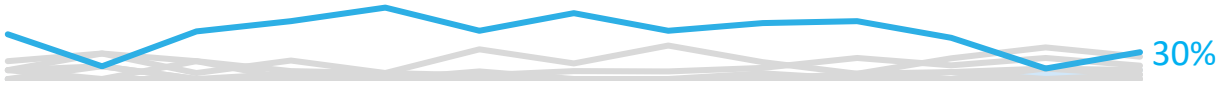
[1] A cyber security incident is a breach of information security in information systems, or a breach of the security and integrity of services or electronic communications networks, resulting from a cybersecurity event.
It is an event that may compromise the confidentiality, integrity, or availability of information systems or networks.
Both terms are defined in the Cybersecurity Act.

Classification of Incidents Reported to NÚKIB

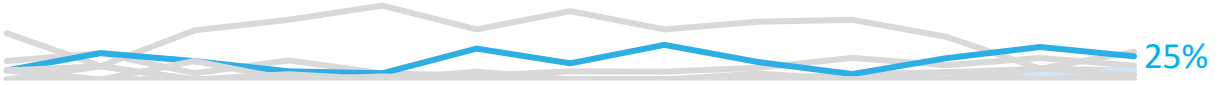
The classification of cyber incident reported to NÚKIB follows the ENISA taxonomy: Reference Incident Classification Taxonomy — ENISA (europa.eu). The graphs below show the monthly distribution of incident categories over the past year. The numerical percentages indicate the proportion of each category relative to the total number of incidents reported in a given month.

2024 **2025**

Availability – e.g. availability disruptions caused by a DoS/DDos attacks or acts of sabotage



Information content security – e.g. unauthorised access to data or unauthorised modification of information



Intrusion – e.g. compromising an application or user account

Malicious Code – e.g. virus, worm, trojan, dialer, spyware

Fraud – e.g. phishing, identity theft or unauthorised use of ICT

Intrusion attempts

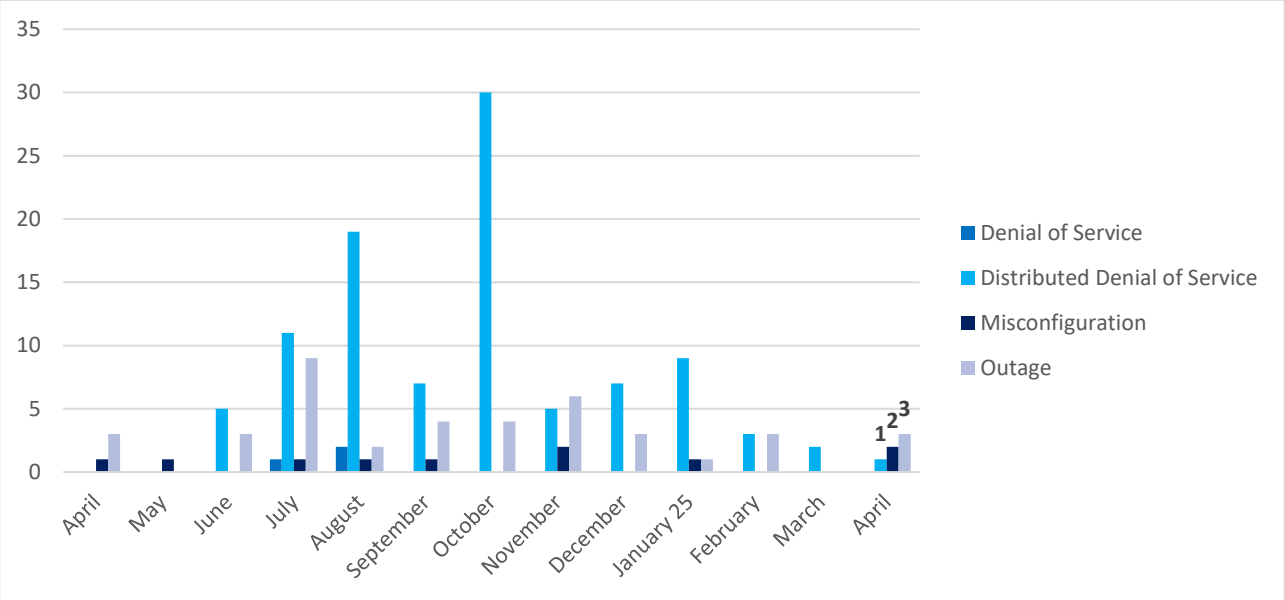
Other

Number of Recorded Incidents in Selected Categories

The categories presented below have been selected due to their long-term frequency (Availability) or severity (Information Security).

Availability

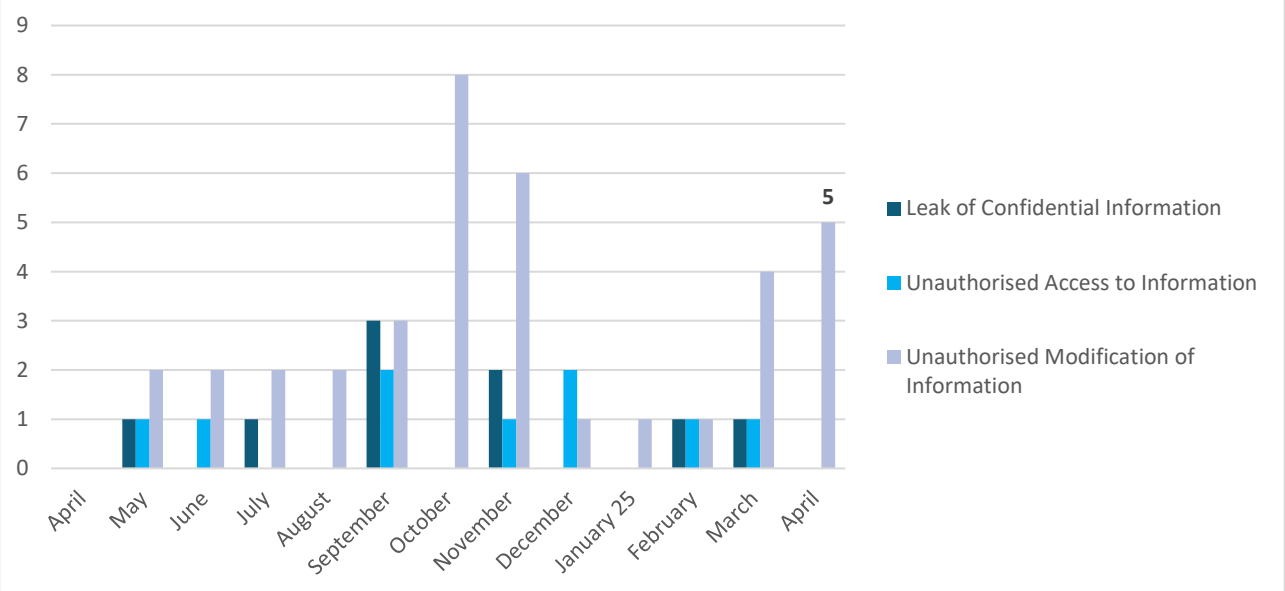
The Availability category primarily includes incidents related to DDoS and DoS attacks. It also covers outages caused by technical failures, misconfiguration or deliberate tampering.



Information Content Security

The Information Security category primarily consists of ransomware attacks, which are typically classified under the subcategory Unauthorized modification of information/data. It

also includes other subcategories such as Unauthorized access to data and systems and Data leak.



Probability terms used

Probability terms and expressions of their percentage values:

Term	Probability
Almost certain	90–100 %
Highly likely	75–85 %
Likely	55–70 %
Realistic probability	40–50 %
Unlikely	15–35 %
Highly unlikely	0–10 %

Traffic Light Protocol

The information provided shall be used in accordance with the Traffic Light Protocol methodology (available at the website https://ww.first.org/tlp/). The information is marked with a flag, which sets out conditions for the use of the information. The following flags are specified that indicate the nature of the information and the conditions for its use:

Colour	Conditions of use
TLP:RED	For the eyes and ears of individual recipients only, no further disclosure. This designation is used when disclosure could pose significant risks to the privacy, reputation, or operations of the organizations involved, and when effective action cannot be taken without such risks. Recipients are therefore strictly prohibited from sharing TLP:RED information with others. For example, in a meeting setting, TLP:RED information may only be shared with those present in the room at the time of disclosure.
TLP:AMBER+STRICT	Restricts sharing to the organization only.
TLP:AMBER	Limited disclosure, recipients may only share this information on a need-to-know basis within their organization and its clients. Sources may use TLP:AMBER when the information requires support to be effectively acted upon, but poses risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.
TLP:GREEN	Limited disclosure, recipients can spread the information within their community. Sources may use TLP:GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: when 'community' is not defined, assume the cybersecurity/defence community.
TLP:CLEAR	Recipients may share this information freely, there are no restrictions on its disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.