Enhancing Cyber Situation Awareness: Visualizing Advanced Persistent Threats as Complex Systems

Georgi Nikolov[1][0000−0002−9020−8408], Margaret Varga[2][0000−0002−9086−1626], April Rose Panganiban[3], Kaur Kullman[4][0000−0001−9480−0583], and Valérie Lavigne[5]

[1] Cyber Defence Lab, Royal Military Academy, Brussels, Belgium
g.nikolov@cylab.be
https://cylab.be
[2] University of Oxford, Oxford, United Kingdom
Margaret.Varga@seetru.com
[3] Air Force Research Laboratory, Dayton, Ohio, USA
april_rose.panganiban@us.af.mil
[4] Center for Space Sciences and Technology, University of Maryland, Baltimore County, Maryland, USA
digilience@coda.ee
[5] Defence R&D Canada, Québec, CANADA
valerie.lavigne@ecn.forces.gc.ca

Abstract. In recent years the field of Information Technologies has become ubiquitous, it is used to implement and manage private, public, government and military installations. This has led to massive growth in the threat landscape, attackers have ample time, resources, technologies and tools to design highly sophisticated attacks implementing Zero-Day Vulnerabilities and complex algorithms using polymorphic behaviour, putting a major strain on defenders. Rapid advancement of Advanced Persistent Threats (APT) poses a major security risk for online services, but even more so for critical government, financial, healthcare and military infrastructures. The difficulty in counteracting APTs is amplified by the increasing challenge of identifying and preparing countermeasures in time. There is ample research and documentation available, describing the life-cycle of various APTs and their Tactics Techniques and Practices (TTPs), but a lack of deeper understanding hinders timely detection to halt the attack. To better understand APTs and how they function, we propose addressing emergent cyber attacks from the perspective of Complex Systems and the application of Visual Analytics and visualization to enhance the level of understanding and Situation Awareness. In this paper, we discuss how we can analyse APTs from a Complex System perspective, the visualization techniques and visual analytics approaches used and how they can be applied for better detection, understanding and management.

Keywords: Advanced Persistent Threat · Complex Systems · Visual Analytics · Visualization · Visual Hierarchy.

1 Introduction

Over the years, our daily lives have become increasingly interconnected, with internet-facing devices enabling a wide range of activities, from streaming content to managing finances and controlling smart homes. Similarly, various infrastructures in healthcare, finance, industry, government, and military sectors have formed a complex cyber environment, enhancing oversight and management. This advancement is driven by new technologies and applications that facilitate connectivity and information exchange.

Despite efforts to manage the new distributed technologies, the growing complexity of integrated systems often leaves vulnerabilities that malicious actors exploit. High-profile attacks on public, private, and government organizations have become common, resulting in infrastructure disruptions and data theft. While many attacks are thwarted by experienced defenders and advanced detection capabilities [1, 32], the proliferation of free tools and information has led to more sophisticated and organized attacks, known as Advanced Persistent Threats (APTs). These threats have become more prominent due to geopolitical instability and technological advancements.

There has been much research on APTs [1, 4, 23], describing how APTs function and possible solutions. APTs are characterized by their stealthy, slow, and meticulous nature, aiming to steal information, conduct espionage, sabotage, or take control of target infrastructures. These threats are carried out by well-organized, often state-sponsored groups with deep knowledge of off-the-shelf applications and ample resources to exploit vulnerabilities. This creates a constant struggle between attackers and defenders, where attackers need only one successful attempt, while defenders must counter every possible attack.

The sophisticated nature of APTs has led to the application of various information technology theories to understand their Tactics, Techniques, and Procedures (TTPs) better. One approach is to model APTs using Complex Systems methodology. This paper explores APTs through the lens of Complex Systems, providing insights into their intricate and dynamic nature. Furthermore, we propose using Visual Analytics and visualization principles to enhance Cyber Situation Awareness [19, 28] for the better understanding and detection of such attacks.

In Section 2, we present our work on applying Complex Systems concepts to APTs. Section 3 discusses how APTs function, their impact, and how to model them as Complex Systems. Our main contribution, detailed in Section 4, is to illustrate ways to understand the cybersecurity domain, particularly APTs, using Visual Analytics and visualization. Multiple practical examples are discussed in Section 4.2, discussing the hierarchy of visualization and how to adapt the information to the intended audience, enhancing awareness at all levels of the hierarchy.

2 Complexity of Cyber Systems

In the Cyber Security Domain, a typical environment often consists of a variety of devices, each with different configurations and purposes, creating a complicated system. Companies use interconnected networks with users working on premises or remotely via a Virtual Private Network (VPN) connection. This creates a complicated infrastructure of a large number of machines that need to be monitored, maintained and managed. By carefully studying the components in the network(s), examining the deployed applications and restricting what can be installed inside the environment, the system administrators can have a good overview and in-depth understanding and knowledge of the network. Problems arise when we add the Human Factor to the equation [13]. By nature, human behaviour is difficult to predict and this is problematic when a high degree of predictability and controllability is required. By including humans as an integral part of a system, it changes from a complicated system to a complex one. This leads to an important shift in operational logic and different tactics need to be applied to manage such an environment [25]. Instead of reducing the system to its smaller simple components, the system needs to be regarded as a whole to detect patterns of emergent behaviour and how it propagates through the system and the non-linear changes it brings. This leads to another important aspect of complex systems: instead of viewing the system as a collection of individual simple components in isolation, it is considered as a "System of Systems". Indeed, a complex system can be composed of various interconnecting sub-systems, varying from simple to complicated or to other complex ones.

2.1 Management of Complex Cyber Systems

Sensitive infrastructures, such as healthcare, financial, industrial, government and military systems, are often the target of malicious actors. The non- deterministic nature of complex systems needs to be taken into account as it can have a severe impact on the stability, resilience, performance and possible vulnerabilities of the environment. These aspects are reinforced by the need for reliable, relevant and precise information to be transferred between segments of the environment in a timely and orderly fashion. Correct interpretation and overview of the environment are imperative for the secure exchange of information. For example, in the military command and control (C2) chain[16], as shown in Fig. 1, an in-depth understanding of the system leads to a high degree of Situation Awareness (SA) for effective decision making [7].

2.2 Situation Awareness in Complex Systems

In its established interpretation, SA was framed as an individual cognitive state that changes based on the dynamics between the human and their environment. Thus SA changes through this interaction and requires maintenance. Endsley's model [7] explains SA maintenance as a cycle, starting from perception of clues

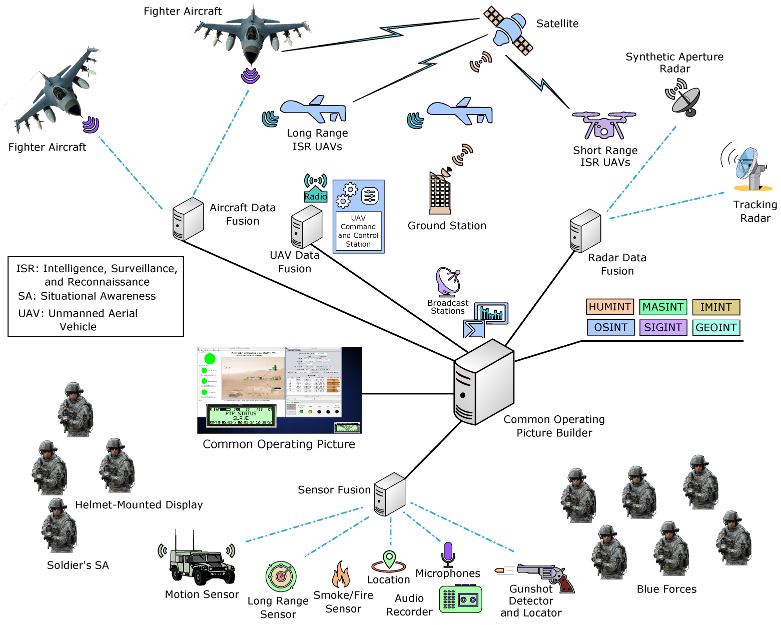


Fig. 1. Overview of military situation awareness as depicted in [16]

from the environment to interpretation of their meaning and resulting in projection of a future outcome. Actions resulting from this process have the ability to change the environment, hopefully creating the desired result for the operator.

However, when SA is incorrect, these actions may create outcomes that result in inaccurate or erroneous projections of the operation, delaying or preventing ideal outcomes. Actions taken under poor SA can add noise to the system, thus adversely affecting future perceptual and interpretation stages of SA maintenance and carrying operators down the wrong decision-making path. Further inaccuracies in SA arise from the complexity of most operational environments where teams work together (adapting the environment) and exchange information. It is acknowledged that team SA is more than the aggregate and overlap of individual SA but arises from the communication between individual members with teammates shaping each other's SA [5]. As operational environments become more complex, a different view of SA is needed to account for the impact of technological advancements in AI. Technology has the ability to aid early stages of SA maintenance and foster team SA through communication aids. Additionally non-human agents form their own situation awareness by monitoring sensors, interpreting data and projecting courses of action to human operators, similarly to human teammates. These Sociotechnical interactions are accounted for in the Distributed Situation Awareness (DSA) model which treats SA as emerging from the interactions between all "agents" in the system (e.g. tools, documents, displays [21]). This approach shows good SA results from using different informational sources (teammates or agents) at the right time and occasionally reverting back to one's individual lens of SA. The DSA view captures how SA occurs in cyber defense and accounts for the complicated process of maintaining it in the presence of new sophisticated threats. Thus, viewing APT attacks and the defense against them as a complex system can directly improve SA for individuals working together in this system.

System intrusions in the form of an APT can lead to skewed, erroneous or often deliberately malicious data being injected into the information flow, perturbing SA. Compromised elements in the system can also be used for data exfiltration of, for example, personal information, threatening the safety of individuals. Malicious actors therefore gain entry to the system at different levels of the system, potentially confusing operators or manipulating their actions by injecting information. The complex nature of a cyber network makes it difficult to maintain awareness across the many connections and levels when threats arise. A better understanding of APTs is needed for proper cyber defense by extending the scope of SA to focus not only on what is happening in the field, but also on how information flows through the system, its origin and its validity.

Countermeasures (i.e., Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Honeypots and the integration of Behaviour-based analysis) are integrated into a Security Information and Event Management (SIEM) architecture for further analysis and correlation. Though intended to assist, the abundance of alerts across various systems combined with time pressure to identify and stop a threat can lead to "alert fatigue" [24] and impairments to SA maintenance in the form of stress and burden on cognitive resources. Vulnerabilities in the operator provide fertile grounds for APTs to continue functioning in the background undetected. Therefore focusing on methods to enhance operator SA maintenance via visualizations and its evaluation [19] may aid in faster resolution of APTs.

3 Advanced Persistent Threats

3.1 Advanced Persistent Threat Definition

First, it is important to clarify the term APT in Information Technologies and literature as most Cyber Threat Intelligence (CTI) sources use APT to refer to organized groups responsible for cyber attacks on high-value targets. However, in scientific literature, APT can also refer to the specific attacks or campaigns by these groups.

In this paper, "APT" denotes a highly sophisticated and targeted cyber attack where an adversary gains unauthorized access and remains undetected for an extended period. APTs involve strategic planning, long-term objectives, and complex execution, often supported by nation-states or well-funded organizations. They are challenging to detect and counter due to dedicated spear phishing attacks, custom malware, and zero-day vulnerabilities. For a more in-depth look, Alshamrani et al. [1] provide an overview of APT techniques and tactics, along with case studies.

Table 1. Examples of APT groups targeting civilian infrastructures [15]

APT Group	**Target Sector**	**Victims**	**Strategy**	**Impact**
APT1 (China)	Commercial/ Industrial	Coca-Cola, Westinghouse	IP Theft, economic espionage	Loss of trade secrets and competitive advantage
APT28 (Russia)	Sports/ Health	WADA, IOC	Data leaks, phishing	Reputation damage, trust erosion
APT10 (China)	IT/ Managed Service	MSPs and client companies	Cloud access, lateral movement	Widespread data theft across sectors
Charming Kitten (Iran)	Academical/ Journalism	Academics, journalists	Credential theft, phishing	Surveillance, compromised communications
Lazarus Group (North Korea)	Media/ Entertainment	Sony Pictures	Destructive malware, data leaks	Operational disruption, public embarrassment
OceanLotus (Vietnam)	Civil Society/ Private Sector	NGOs, companies, media	Watering hole, document malware	Espionage, surveillance
APT33 (Iran)	Aviation/ Energy	Aerospace, energy firms	IP Reconnaissance, malware	Preparation for sabotage, IP theft

To illustrate the impact of APTs on different infrastructures, examples of attacks on the civilian sector are presented in Table 1. It is important to note that the information on these groups is source-dependent and often comes with a degree of vagueness.

3.2 APTs from a complex system perspective

As discussed previously, Advanced Persistent Threats are highly sophisticated attacks, often perpetrated by well-organized groups. More often than not, these groups are state sponsored, which leads to their targets often being financial, government or military.

Major effort has been done in the field of CTI to identify and collect information about APTs. Initially, a definition of their life cycle was proposed in the form of the Cyber Kill Chain [33], later expanded by MITRE [15, 22]. Platforms such as MITRE ATT&CK and MISP [31] offer a large collection of data, pertaining to the TTPs of APTs. All this information is often in text form, which requires long period of time to process and identify the key characteristics of advanced threats. Through the use of Knowledge Graphs [10], we can shorten this time and represent in a visual way the different APTs, offering a high degree of data exploration and analysis. This is shown in Fig. 2, a high level view of techniques used and their mitigation procedures.

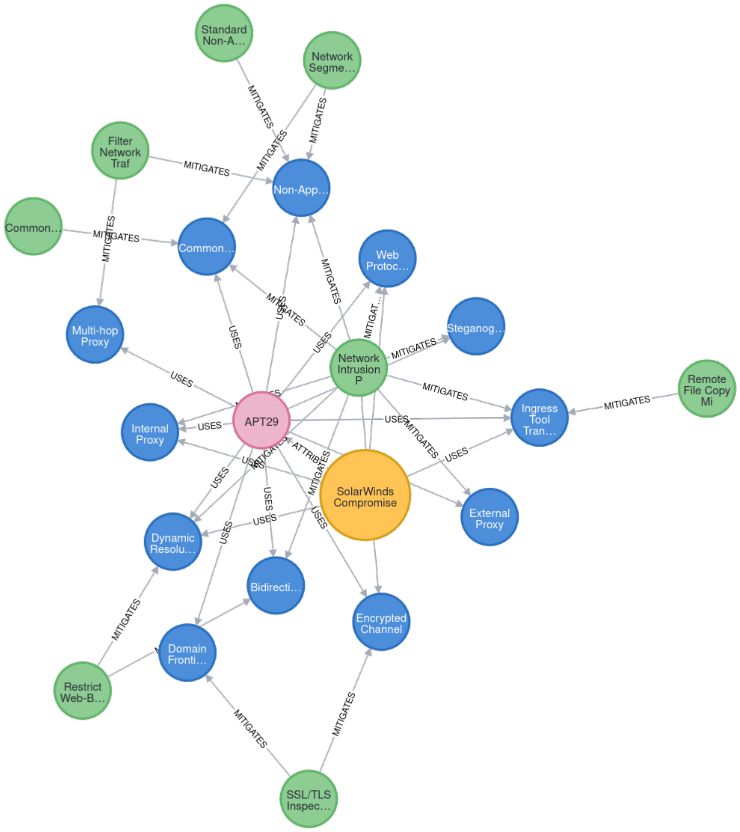


Fig. 2. Knowledge Graph representation of APT29 and SolarWinds Compromise

The Knowledge Graph representation gives us a good high level overview, but to better understand how APTs work, we also need a way to follow the life cycle of a specific attack, as shown in Fig. 3, visualizing the initial stages and how they interconnect. For this example, we chose to represent the SolarWinds APT [32].

Each phase of the attack, from Reconnaissance to Resource Development, relies on previously gathered information and decisions. Social engineering is crucial in the initial phases, as humans are the weakest link in any complex system. While regulations secure hardware and software, the Human Factor remains unpredictable. The vast amount of daily information produced in hybrid networks can put a lot of strain Security Operations Center (SOC) members. Sophisticated attacks often mimic benign activity, generating many false positives and true detections. This constant vigilance can lead to "Vigilance Decrement" reducing Situation Awareness (SA) and weakening detection [8].

To help mitigate this strain, a better understanding of APTs is needed, leading to quicker identification and detection of malicious activity. Modeling an

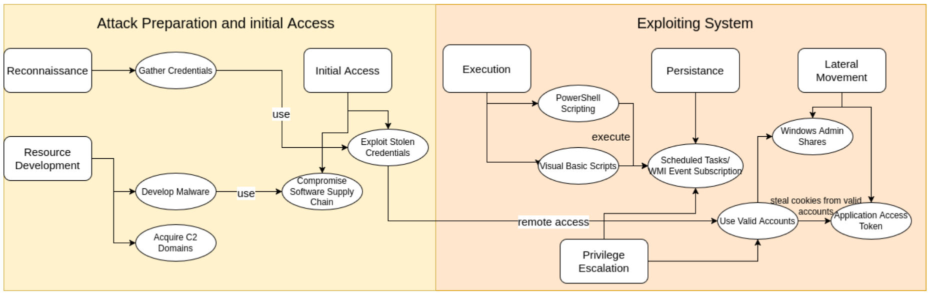


Fig. 3. Graph representation of the initial stages of the SolarWinds APT attack, based on data from MITRE ATT&CK

APT as a complex system, there are four distinct levels we need to focus our attention on- the micro, meso, macro and meta levels. The four levels are part of the "system-based" approach for enhanced monitoring and management of the interactions and emergent behavior [25, 26]. Each of these levels not only describes the scope of observation, but also has distinct characteristics and interactions within, and with other levels.

The Micro Level, Individual actors & Attack vectors At the micro level, APTs focus on individual actions, starting with reconnaissance and using gathered information to create entry vectors. Social engineering is crucial in the initial stages, as demonstrated by SolarWinds [32], which combined social engineering and software supply chain attacks for initial access. Collecting user credentials through spear phishing, password spraying, and API abuse sets the attack in motion, leading to significant consequences due to system interdependence. This illustrates the non-linearity of complex systems- attackers adapt based on feedback from phishing victims or system defenses, leading to emergent behavior. Feedback loops are evident as attackers learn from public information and modify strategies to bypass security measures.

The Meso Level, Organizational Systems & Infrastructure The meso level focuses on organizational systems, IT infrastructure, human elements, and internal security. Current infrastructures are tightly coupled and interconnected to facilitate data sharing and management, which can be beneficial but also exploitable by attackers. The SolarWinds attack exemplifies this, where attackers inserted a backdoor via a management product's software supply chain, making any network machines using the compromised software easy targets.

Large networks have numerous interconnected machines and applications, ranging from generic to highly specialized. Defending this vast array of potential targets is challenging, as minor vulnerabilities can initiate a cascade of system-wide issues. Incident response must be well planned and documented, as new attack vectors may emerge during the response. Defensive measures prompt attackers to evolve new methods to stay hidden and continue compromising the system.

The Macro Level, National/Global Systems & Ecosystems At the macro level, the focus shifts to national and global networks, industry-wide interactions, and the regulatory environment. The Ukraine Electric Power attacks [3] illustrate the non-linearity of APTs, where attacking electrical infrastructure during war-time causes national-scale ripple effects, impacting civilians, government institutions, hospitals, and military operations. The interdependency of national and global systems can enhance resilience through faster information and resource exchange but also create systemic vulnerabilities. International regulatory changes and responses to cyber attacks influence future attack strategies, exemplifying the complex feedback loops in the global system.

The Meta Level: Sociopolitical, Economic & Technological Context Advanced cyber attacks significantly impact societal, political, and economic landscapes. Economic growth can make a country a target for financial gain, while political interests can drive disinformation campaigns using APTs to steal information or damage opposition. Military institutions are prime targets for financial or strategic gains. The evolving sociopolitical, economic, and technological landscape leads to new forms of cyber warfare, shifting global power dynamics and initiating retaliatory measures and technological arms races.

APT System Levels interaction Each of the levels exhibits Feedback Loops, representing behavioral change within each specific scale. Furthermore, significant interactions between the different levels serve as feedback in between layers. This is represented in Fig. 4, showing the interaction between the different layers.

Micro-level breaches (e.g. phishing) impact the meso-level organizational structure. In response, the attackers will adapt their approach at the micro-level based on the aforementioned changes. Any vulnerabilities within one organization can propagate to industry-wide impacts and new defensive measures will lead to the implementation of new TTPs by adversaries. Further, national cyber strategies influence global cyber conflicts, shifting the power balance one way or another, which leads to the creation of new international agreements, or the

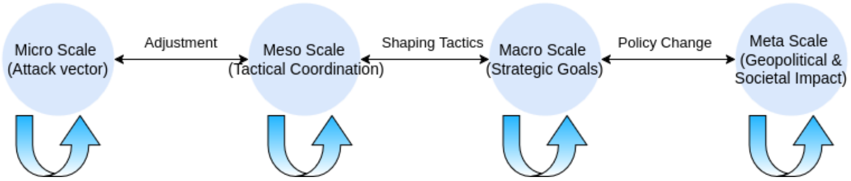


Fig. 4. Visual representation of the interactions between the different levels and the Feedback Loops inherent to the various levels

break up of old ones, shaping the development of cyber capabilities for specific industries and environments.

4 Visualizing APTs as Complex Systems

The primary challenge in dealing with APTs is their detection, as they aim to remain hidden for extended periods for espionage, exfiltration, and sabotage. Analysts often use various tools to review the vast amount of network data for anomalies, but data heterogeneity complicates this task. Effective data visualization and the application of Visual Analytics can enhance Situation Awareness (SA) by representing different types of information uniformly, aiding in the identification and understanding of malicious activity [27]. Visual Analytics offers several advantages for APT awareness, including enhanced detection, discovery of hidden patterns, and transformation of raw data into intuitive visual representations, facilitating faster and more efficient decision-making [18]. Historical data and predictive models also support proactive defense strategies, while interactive visualizations improve communication and collaboration among stakeholders.

It is crucial to consider the intended audience for these visualizations, determining the appropriate level of detail and the message to be conveyed. The four levels described in Section 3.2 should be translated into visual forms that match the audience's experience and SA level.

4.1 Hierarchy of the APT visualization

Selecting the appropriate visualization for cyber information depends on the users' knowledge, experience, objectives, tasks, and work environment. Users at different levels (micro, macro and above) require different views, and no single interface can address all needs. This is especially true in the military domain, where

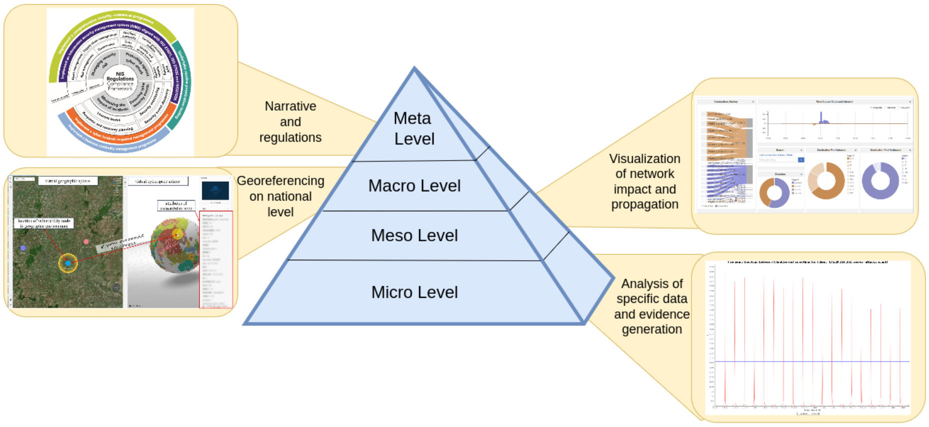

NIS Regulations Compliance Framework
Narrative and regulations
Meta Level
Macro Level
Meso Level
Micro Level
Georeferencing on national level
Visualization of network impact and propagation
Analysis of specific data and evidence generation

Fig. 5. Representing APT information at different levels of visualization [11][17]

rapid and precise information comprehension is crucial for the advancement of mission objectives. Incorporating new forms of cyber symbology, as discussed in [29], can bridge data representation across levels and facilitate information exchange.

The four levels of Complex Systems described in Section 3.2 can be visualized as a pyramid, with the micro level at the base and the meta level at the top. Fig. 5 illustrates this, highlighting that most work in identifying and understanding APTs occurs at the micro level. At the micro level, analysts sift through data to detect abnormalities and indicators of suspicious activity, using proxy logs, network packets, endpoint logs, and other data types. Visualizations must offer functionalities to compare, filter, correlate, and dive deeper into the data [12]. As we move up the pyramid, data abstraction must match the intended audience's level of Situation Awareness (SA). The meso level will correlate data from individual end-points and create a high level overview of the network and the impact on the infrastructure. At the macro level, the gathered information needs to be abstracted so it can be applied to various infrastructures on national level. Finally, at the meta level, the impact on the sociopolitical and economical level needs to be evaluated. For each of the levels, the information needs to be adapted to suit the user's needs and goals. Even though the information is abstracted, moving through the levels provides greater awareness of the system structure and the connections between levels.

4.2 Practical Examples of APT hierarchy visualization

To better understand how Visual Analytics can be applied for APT detection, a collection of examples will be presented for each hierarchical level. The focus at

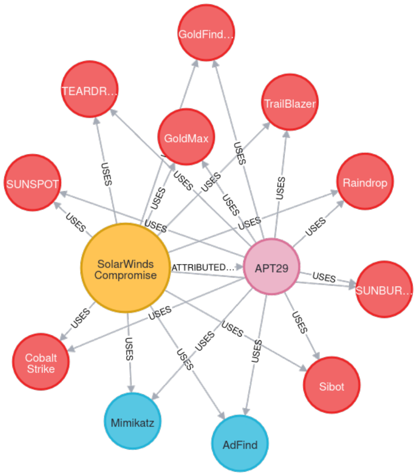
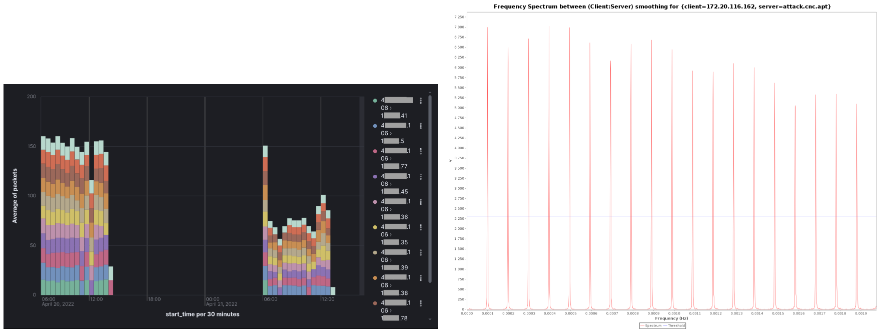


Fig. 6. Knowledge Graph representation of the SolarWinds malwares and tools used



(a) (b)

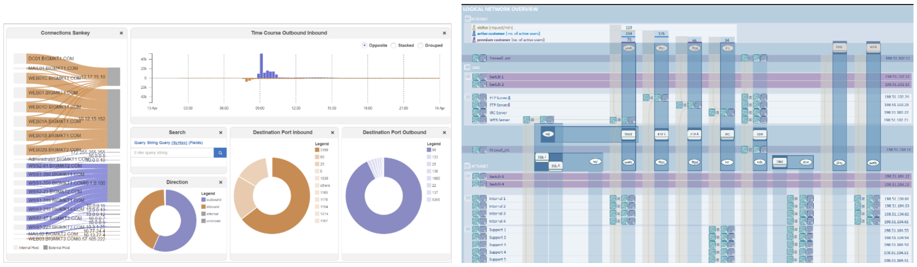
Fig. 7. (a) Bar graph visualization of netflow connections (b) Frequency spectrum visualization

each scale is very different and highly dependant on the user's area of expertise and the SA level.

Micro Level The micro level focuses on specific points in the network, be that a specific connection, machine or application. The goal is to determine the cause of the abnormal behavior, following the chain of effect back from the malicious instance, discovered in the network. To do that, often analysts will focus on program execution, netflow and proxy logs.

A Knowledge Graph, as shown in Fig. 6, visually represents the APT, malware, and associated tools, aiding analysis of process execution on host machines. With AI detection tools, Knowledge Graphs are useful for both data exploration and model training.

When analyzing the flow of information in a network, the analyst must focus on specific connections established by internal hosts or internal machines and external servers. This is not always evident as in a day, thousands of connections are established. It is not easy to single out the suspicious ones for analysis, so to identify malicious connections, analysts often look for patterns that are abnormal in nature. These patterns are defined by characteristics such as periodicity, ports used, quantity of data exchanged, geo-location, etc. In Fig. 7, two examples of pattern visualizations are shown. In Fig. 7 (a) is a representation of the packet traffic between internal machines and a suspicious external server. The bar chart displays multiple characteristics of the connections such as the protocols used, duration of the connection and bytes exchanged. The information is shown for the duration of two days- this can be used to see if there is repetition and if there are common characteristics between the different connections. As shown in the figure, there seems to be a high degree of similarity between the various connections in regards to the number of packets exchanged and the frequency of connections. Regarding the frequency, Fig. 7 (b) showcases a more specialized visualization, focused on representing the frequency of a specific connection



(a) (b)

Fig. 8. (a) Scanning/probing activities on multiple clients in the network [30] (b) System level overview of machines in the network [30]

between a client and an external server. The frequency spectrum is a transformation of time-based data into the frequency domain aiming to detect certain periodicity spikes. APTs often use predetermined periodic time intervals of connection between an infected host and the C2 server to fetch new commands or exfiltrate information. By detecting these periodic connections, we can better pin-point clients that need to be further investigated.

Meso Level The meso level aims to describe the emergent behavior and feedback loops present on the organizational and infrastructure layer. Instead of focusing on a specific slice of data or one host in the network, the view is zoomed out to observe the network as a whole and the emergent behavior therein. Fig. 8 shows how we can represent the network in two ways- Fig. 8 (a) a dashboard representation visualizes the scanning and probing activities that have been observed in the network. Such visualizations are useful to better discern anomalous

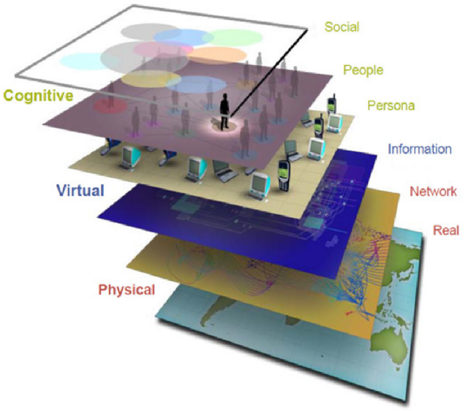


Fig. 9. Layered view of cyberspace. [20]

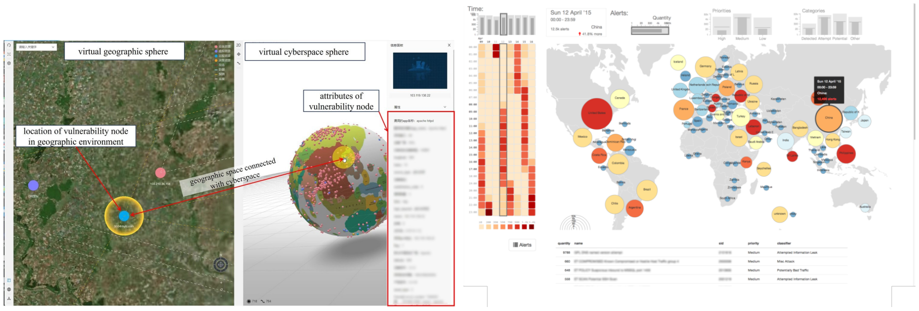
behavior by comparing activities between clients and observing the evolution in time. To better asses how different machines in the network act, a visualization such as in Fig. 8 (b) can be useful- here a representation of the system helps to better visualize how the machines interact and their function in the system. Fig. 8 (a) is a user-centric based visualization where the user's experience and knowledge is leveraged to better understand the situation in the network. In Fig. 8 (b) a system-based approach helps to better understand how the system functions as a whole and the impact the emergent behavior may have on it.

Macro Level At the macro level, there is value in leveraging concepts from the Activity Based Intelligence methodology [2]. More specifically, we want to leverage the concept of georeferencing to discover, i.e. to focus on spatially and temporally correlating data to discover key events, trends and patterns.

It is helpful to consider the multiple layers of the cyberspace shown in Fig. 9. Jiang et al. [11] proposed to visualize the multiple layers of cyber information, including meta level command and control relationship through a geo-cyber metaphor that can be represented with knowledge graphs and linked to the geographic environment (see Fig. 10 (a)).

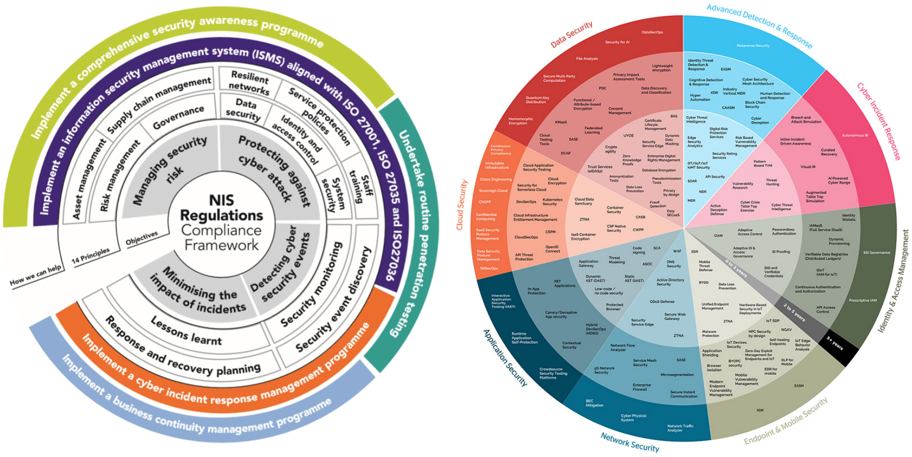
Another example of geospatial visualization related to the cyber space is BubbleNet [14], as shown in Fig. 10 (b). It was designed as a cyber security dashboard to enable patterns identification and summarizations for users beyond network analysts, such as network managers.

Meta Level As the meta level involves a wide range of information covering the sociopolitical, economic and technological contexts, multiple visualizations are required. At this level, we may be interested in visualizing the legal context surrounding the cyber environment. In some cases, meta level information regarding politics, legal aspects, cultural environment, and human involvement


virtual geographic sphere
virtual cyberspace sphere
attributes of vulnerability node
location of vulnerability node in geographic environment
geographic space connected with cyberspace
Time:
Sun 12 April '15
Alerts:
Quantity
China
Priorities
Categories
Alerts

(a) (b)

Fig. 10. (a) Visualizing the geo-cyber space with a geo-cyber metaphor represented with multi-layer knowledge graphs. [11] (b) BubbleNet dashboard example. [14]


Implement a comprehensive security awareness programme
Implement an information security management system (ISMS) aligned with ISO 27001, ISO 27035 and ISO27036
Undertake routine penetration testing
Implement a cyber incident response management programme
Implement a business continuity management programme
Asset management
Risk management
Supply chain management
Governance
Resilient networks
Data security
Service protection policies
Identity and access control
System security
Staff training
Managing security risk
Protecting against cyber attack
Detecting cyber security events
Minimising the impact of incidents
Security monitoring
Security event discovery
Lessons learnt
Response and recovery planning
NIS Regulations Compliance Framework
Objectives
14 Principles
How we can help
Data Security
Advanced Detection & Response
Cyber Incident Response
Identity & Access Management
Endpoint & Mobile Security
Network Security
Application Security
Cloud Security

(a) (b)

Fig. 11. (a) NIS Regulations: Cyber Assessment Framework. [17] (b) Cybersecurity tech radar. [6]

could be represented as knowledge graphs linked to geographical spaces (often at country-level precision) and also visualized using the geo-cyber metaphor [11].

Regarding the technological perspective, infographics representing the regulatory space and the cybersecurity technological landscape can give a quick visual summary of this information. The NIS regulatory framework is depicted in Fig. 11 (a) from [17] through the use of concentric circle arcs that convey the hierarchical categorisation of the regulation framework. An example of technological cybersecurity context visualization is provided in Fig. 11 (b) from [6], where it is represented as a pie chart combining circle arcs divided by functions and a radial axis for expected temporal information.

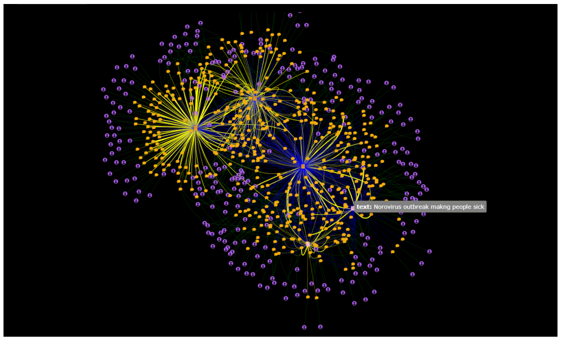


Fig. 12. HAITTON Knowledge graph view, linking posts and online actors to key narratives of interest. [9]

The sociopolitical landscape involves narratives that surround cyber events, which are often discussed online within social media and discussion forums. For example, the HAITTON application (see Fig. 12) helps track and visualize online narratives [9].

5 Conclusion

The success of an APT arises from the interaction of actions across micro, meso, macro, and meta scales, exploiting the interconnectedness of modern systems to create cascading effects and emergent outcomes. This emergent behavior is far more impactful than the sum of individual actions.

A complex systems perspective on APTs enhances understanding of their behaviors, enabling better detection, prevention, and resilience. This approach shifts focus from reactive measures to proactive, systemic solutions, addressing the interdependent and adaptive nature of cyber threats. Supporting proactive behavior requires enhanced SA of the APT's entry into and activity within the larger system. Examining feedback loops from both the attacker's and defender's viewpoints provides a dynamic insight of how APTs unfold, evolve and adapt. These perspectives reveal how actions and reactions at different scales direct escalation or containment, often in an unpredictable manner. Feedback loops within and between scales are critical to understanding the dynamic nature of these attacks. These loops enable adaptation, amplify effects, and create emergent behaviours. Through the understanding of APTs as complex, multi-scale phenomena, organizations can design defences that are adaptive and resilient to the long-term, sophisticated nature of these threats. Visualizations aimed at categorizing the different levels of the network assist in identifying cues, interpreting the extent of their impact across the entire system and allow for appropriate solutions. Additionally, they support a larger DSA view, where deeper understanding can be gained of the meso and meta scale components affected by a particular APT. This larger scale awareness of the impact of new APTs on a system can benefit detection from human operators and allow them to better train AI detection.

6 Future Work

In this paper, we have presented our work in the field of Complex Systems, its importance for the appropriate understanding and management of large-scale hybrid infrastructures. Further, through the application of complex system principles to the field of Advanced Persistent Threats, new ways are proposed for the application of Visual Analytics for their detection, developing new visualization techniques to enhance the Cyber Situation Awareness and bridge the gap between the levels of visualization hierarchy. Finally, specific evaluation techniques are needed for the assessment of the usefulness and usability of the visual tools, alongside methods for the correct evaluation of SA and its validity.

Acknowledgments. This is the work of the NATO Visual Analytics for Complex Systems Research Task Group.

References

1. Alshamrani, A., Myneni, S., Chowdhary, A., Huang, D.: A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. IEEE Communications Surveys & Tutorials **21**(2), 1851–1877 (2019)
2. Atwood, C.P.: Activity-based intelligence: Revolutionizing military intelligence analysis. Joint Force Quarterly **77**(2nd Quarter) (2015)
3. Case, D.U.: Analysis of the cyber attack on the ukrainian power grid. Electricity information sharing and analysis center (E-ISAC) **388**(1-29), 3 (2016)
4. Chen, P., Desmet, L., Huygens, C.: A study on advanced persistent threats. In: Communications and Multimedia Security: 15th IFIP TC 6/TC 11 International Conference, CMS 2014, Aveiro, Portugal, September 25-26, 2014. Proceedings 15. pp. 63–72. Springer (2014)
5. Cooke, N.J., Gorman, J.C., Winner, J.L., Durso, F.: Team cognition. Handbook of applied cognition **2**, 239–268 (2007)
6. Eviden (2025), https://eviden.com/publications/tech-radar/cybersecurity/
7. Endsley, M.R., Connors, E.S.: Situation awareness: State of the art. In: 2008 IEEE Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century. pp. 1–4. IEEE (2008)
8. Grier, R.A., Warm, J.S., Dember, W.N., Matthews, G., Galinsky, T.L., Szalma, J.L., Parasuraman, R.: The vigilance decrement reflects limitations in effortful attention, not mindlessness. Human factors **45**(3), 349–359 (2003)
9. Riskaware (2025), https://www.riskaware.co.uk/insight/harnessing-the-power-of-ai-for-tracking-harmful-online-narratives/
10. Hogan, A., Blomqvist, E., Cochez, M., d'Amato, C., Melo, G.D., Gutierrez, C., Kirrane, S., Gayo, J.E.L., Navigli, R., Neumaier, S., et al.: Knowledge graphs. ACM Computing Surveys (Csur) **54**(4), 1–37 (2021)
11. Jiang, B., You, X., Li, K., Li, T., Wang, X., Si, D.: Virtual geo-cyber environments: metaphorical visualization of virtual cyberspace with geographical knowledge. International Journal of Digital Earth **17**(1), 2324959 (2024)
12. Liggett, K., Kullman, K.: Chapter 2 – human factors considerations for visual analytics, exploratory visual analytics. Tech. Rep. 10.14339/STO-TR-IST-141, NATO (February 2023)
13. Marble, J.L., Lawless, W.F., Mittu, R., Coyne, J., Abramson, M., Sibley, C.: The human factor in cybersecurity: Robust & intelligent defense. Cyber Warfare: Building the Scientific Foundation pp. 173–206 (2015)
14. McKenna, S., Staheli, D., Fulcher, C., Meyer, M.: Bubblenet: A cyber security dashboard for visualizing patterns. In: Computer Graphics Forum. vol. 35, pp. 281–290. Wiley Online Library (2016)
15. Mitre att&ck (2024), https://attack.mitre.org/
16. Munir, A., Aved, A., Blasch, E.: Situational awareness: techniques, challenges, and prospects. AI **3**(1), 55–77 (2022)
17. Nis (2025), https://www.ncsc.gov.uk/collection/cyber-assessment-framework/caf-supplementary-information
18. Nikolov, G., Debatty, T., Mees, W.: Detection through visualization for the multi-agent system for apt detection. In: Digital Transformation, Cybersecurity,

And Resilience DIGILIENCE 2022 (2022), https://cylab.be/publications/43/2022-detection-through-visualization-for-the-multi-agent-system-for-apt-detection

19. Nikolov, G., Perez, A., Mees, W.: Evaluation of cyber situation awareness-theory, techniques and applications. In: Proceedings of the 19th International Conference on Availability, Reliability and Security. pp. 1–10 (2024)
20. Parish, M., Madahar, B.: Understanding cyberspace through cyber situational awareness. The Defence Science and Technology Laboratory: Wiltshire, UK (2016)
21. Stanton, N.A., Salmon, P.M., Walker, G.H., Salas, E., Hancock, P.A.: State-of-science: situation awareness in individuals, teams and systems. Ergonomics **60**(4), 449–466 (2017)
22. Strom, B.E., Applebaum, A., Miller, D.P., Nickels, K.C., Pennington, A.G., Thomas, C.B.: Mitre att&ck: Design and philosophy. In: Technical report. The MITRE Corporation (2018)
23. Tankard, C.: Advanced persistent threats and how to monitor and deter them. Network security **2011**(8), 16–19 (2011)
24. Tariq, S., Baruwal Chhetri, M., Nepal, S., Paris, C.: Alert fatigue in security operations centres: Research challenges and opportunities. ACM Computing Surveys **57**(9), 1–38 (2025)
25. Traeber-Burdin, S., Varga, M.: How does systems thinking support the understanding of complex situations? In: 2022 IEEE International Symposium on Systems Engineering (ISSE). pp. 1–7. IEEE (2022)
26. Träber-Burdin, S., Varga, M.: Dealing with complex situations: towards a framework of understanding problems. In: 2022 IEEE International Conference on Systems, Man, and Cybernetics (SMC). pp. 1431–1436. IEEE (2022)
27. Varga, M., Winkelholz, C., Träber-Burdin, S., Bivall, P., Kullman, K.: Chapter 7 cyber situation awareness, exploratory visual analytics. Tech. Rep. 10.14339/STO-TR-IST-141, NATO (February 2023)
28. Varga, M., Winkelholz, C., Traber-Burdin, S.: Cyber situation awareness. NATO/OTAN (STO-MP-IST-148) (2016)
29. Varga, M., Winkelholz, C., Träber-Burdin, S.: An exploration of cyber symbology. In: 2019 IEEE Symposium on Visualization for Cyber Security (VizSec). pp. 1–5. IEEE (2019)
30. Varga, M., Winkelholz, C., Traeber-Burdin, S.: Exploration of user centered and system based approaches to cyber situation awareness. environment **1**, 2 (2018)
31. Wagner, C., Dulaunoy, A., Wagener, G., Iklody, A.: Misp: The design and implementation of a collaborative threat intelligence sharing platform. In: Proceedings of the 2016 ACM on workshop on information sharing and collaborative security. pp. 49–56 (2016)
32. Wolff, E.D., GroWlEy, K.M., Lerner, M.O., Welling, M.B., Gruden, M.G., Canter, J.: Navigating the solarwinds supply chain attack. Procurement Law. **56**, 3 (2021)
33. Yadav, T., Rao, A.M.: Technical aspects of cyber kill chain. In: Security in Computing and Communications: Third International Symposium, SSCC 2015, Kochi, India, August 10-13, 2015. Proceedings 3. pp. 438–452. Springer (2015)