Military Cyber Affairs

Volume 7
Issue 1 *HammerCon 2024 Issue*

Article 5

May 2024

Characterizing Advanced Persistent Threats Through the Lens of Cyber Attack Flows

Logan Zeien
University of Colorado, Colorado Springs (UCCS), lzeien@uccs.edu

Caleb Chang
University of Colorado, Colorado Springs (UCCS), cchang@uccs.edu

LTC Ekzhin Ear
University of Colorado, Colorado Springs (UCCS), eear@uccs.edu

Dr. Shouhuai Xu
University of Colorado, Colorado Springs (UCCS), sxu@uccs.edu

Recommended Citation

Zeien, Logan; Chang, Caleb; Ear, LTC Ekzhin; and Xu, Dr. Shouhuai (2024) "Characterizing Advanced Persistent Threats Through the Lens of Cyber Attack Flows," *Military Cyber Affairs*: Vol. 7 : Iss. 1 , Article 5.
Available at: https://digitalcommons.usf.edu/mca/vol7/iss1/5

Characterizing Advanced Persistent Threats Through the Lens of Cyber Attack Flows

Cover Page Footnote

This publication was supported by Award Number SA10012022020481 from the Griffiss Institute for VICEROY program. Its contents are solely the responsibility of the authors and do not necessarily represent the official views of the sponsor.

Characterizing Advanced Persistent Threats through the Lens of Cyber Attack Flows

Logan Zeien, Caleb Chang, LTC Ekzhin Ear, and Dr. Shouhuai Xu

Executive Summary

Effective cyber defense must build upon a deep understanding of real-world cyberattacks to guide the design and deployment of appropriate defensive measures against current and future attacks. In this abridged paper (of which the full paper is available online), we present important concepts for understanding Advanced Persistent Threats (APTs), our methodology to characterize APTs through the lens of attack flows, and a detailed case study of APT28 that demonstrates our method's viability to draw useful insights. This paper makes three technical contributions. First, we propose a novel method of constructing *attack flows* to describe APTs. This abstraction allows technical audiences, e.g., defensive cyber operators, to parse and infer valuable details, while allowing management- and business-minded audiences to holistically visualize the attacks' progression without being overwhelmed by technical details. Second, we provide a case study on a real-world APT to demonstrate the effectiveness of our attack flow methodology that systematizes cyberattack tactics, techniques, and procedures. This technical characterization potentially can, for example, train machine learning models to detect and recognize such cyberattacks automatically. Third, we show that the attack flow representation also allows us to draw insights into the strengths, weaknesses, impact, and sophistication of APTs, as well as to identify potential mitigation approaches. We find that APT28 tends to employ unsophisticated techniques when possible and the root cause for APT28's success is social engineering. The full version of this paper details additional case studies and comparative analysis of multiple APTs, leading to further insights.

Introduction

Cyberattacks are increasing in sophistication. Advanced Persistent Threats (APTs) demonstrate this trend, consistently conducting well-prepared and orchestrated attacks, which often advance nation-state objectives. Consequently, cyber defenders must understand real-world APT cyber campaigns to derive effective defensive strategies and technical mechanisms to safeguard their networks and systems. Cyber threat analysts regularly analyze real-world APTs to produce Cyber Threat Intelligence (CTI) reports to inform security teams, managers, and executives. However, such reports often require significant time and domain expertise to holistically understand the cyber incident (cf. CrowdStrike Intelligence, 2022). Otherwise, the reports may convey sweepingly generalized information too shallow to meaningfully derive practical cyber defense mechanisms (Huntley, 2022; UK Government, 2021). These unsatisfying situations prompt us to seek a more intuitive method for describing sophisticated APT cyber activities. In this abridged paper (the full version is available online), we propose such a method to support both technical audiences (practitioners who implement cyber defense mechanisms), and management audiences, (cyber defense decision makers).

Concepts

Cyberattack Tactic, Technique, and Procedures (TTP)

The MITRE Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) framework is commonly used in the industry by cyber threat and digital forensics analysts to describe real-world cyber incidents in terms of *tactics*, *techniques*, and *procedures*, which MITRE defines as follows (Strom et al., 2018):

- Cyberattack *tactic* identifies an attacker’s objective or sub-objective. This concept corresponds to operational objectives as described in U.S. Army doctrine for kinetic operations (U.S. Army, 2016). For example, the Reconnaissance tactic (TA0043) intended to identify the vulnerabilities of a network firewall appliance in a cyber operation corresponds to a kinetic operation where a cavalry unit conducts reconnaissance on an enemy’s perimeter defense to identify potential vulnerabilities or gaps.

- Cyberattack technique identifies the method for achieving a cyberattack tactic. This concept is analogous to the idea of tactical tasks in Army doctrine (Ibid.). For example, the Brute Forcing technique (T1110), where an attacker executes a dictionary payload against a network firewall to see what vulnerabilities may surface, corresponds to the cavalry unit conducting reconnaissance by fire, namely launching kinetic payloads at various locations around the enemy perimeter to see how the enemy reacts.

- Cyberattack procedure is a technical instantiation of a cyberattack technique and produces observable behaviors. This concept is like battle drills in Army doctrine (Ibid.). For example, an attacker may use the Hydra brute-forcing utility against network firewalls; this corresponds to an infantry Weapons Company engaging the enemy perimeter with 60mm mortars while a cavalry unit observes from overwatch positions.

The Concept of Cyberattack Flow

The concept of attack flow was implicitly introduced as *cyberattack narratives* in (Mireles et al., 2016) and then formally introduced in (Ear et al., 2024a) to describe the system and network components (e.g., computers or devices) that an adversary progressively compromises during an attack. In this paper, we extend the concept to describe further the tactics and techniques attackers employ in relation to the compromised victim assets. An APT may have multiple attack flows as a part of their cyber operation campaign.

Using attack flows to analyze cyber incidents is more helpful than using ATT&CK and Lockheed Martin's Cyber Kill Chain to list techniques because attack flows provide the ability to visualize the sequence and progression of cyber activities. Continuing with the previous example, we can place the Brute Forcing technique (T1110) against a firewall in the context of an attack flow for the overall cyber operation to gain Initial Access to a victim's internal network, Laterally Move to a data-rich server, and Exfiltrate the sensitive data. Correspondingly, the kinetic concept of reconnaissance by fire conducted by the cavalry unit may be part of a kinetic operation where their scheme of maneuver is to penetrate the enemy assembly area, locate the enemy's battle plans, and retrieve it.

Methodology

To understand APTs through the lens of attack flows, we introduce the following three-step methodology: (i) characterizing cyber campaigns in terms of attack flows, encompassing their associated TTPs; (ii) evaluating the strengths and weaknesses of an APT; and (iii) analyze the impact, sophistication, and potential mitigations for an APT to draw insights. These steps are elaborated below.

To characterize the cyberattacks waged by APTs, our method takes CTI reports, along with ATT&CK's matrix of techniques, to construct attack flows. Note, this method can be extended for non-IT networks by leveraging, for example, Aerospace Corporation's framework when the space segment is involved (Ear et al., 2024a; Ear et al., 2023). Raw reports contain vital forensics-level details for cyberattack procedures, and processed reports fill in gaps where raw reports are not publicly available. We propose extracting from these reports: (i) the victim computers and/or components, which formulate the vertex set in attack flows; and (ii) the techniques that attackers select to progress from one compromised vertex to the next vertex, which correspond to the arcs in attack flows. Thus, we obtain an attack flow representation of an APT.

To analyze the strengths and weaknesses of an APT, we consider the characteristics of their attacks in terms of their ability to achieve their tactics, how effectively they progress across the victim systems and networks, their versatility in delivering cyber capabilities, and their ability to evade or overcome defensive cyber mechanisms.

Our method characterizes each APT's impact, sophistication, and mitigations. Impact is described from four perspectives: (i) *financial*, characterized by financial theft and cost of recovery; (ii) *data*, namely the volume and sensitivity of data exfiltration; (iii) *publicity*, a qualitative characterization; and (iv) *operation*, namely disruptions to the victims' network operations. Sophistication is characterized from three perspectives: (i) *attack flow difficulty*, such as the depth of the attack flow or evaluated defense of the victim's network; (ii) *attack novelty*, such as the uniqueness or variance of the attack flow and procedures; and (iii) *demonstrated resources employed*, such as the Command and Control (C2) infrastructure or pool of procedures for achieving a common technique. Mitigations are identified by analyzing the root causes in APT attack flows, where each root cause is ideally an attack technique that enabled the attack.

Characterizing a Real-World APT through the Lens of Attack Flows

In this section we present a case study of APT28, one of the most sophisticated cyber threat groups, to demonstrate our method's viability. We introduce the background of APT28, describe its attack against U.S. Democratic Committees, and provide the results of our technical work in constructing APT28's corresponding attack flows. Using these attack flows, we characterize APT28's strengths, weaknesses, impact, and sophistication. Finally, we present mitigations derived from the attack flows.

Background of APT28

APT28, also known as Fancy Bear, is a reportedly a Russia-sponsored threat group involved in data exfiltration and espionage. The main objective of APT28 is to disclose sensitive data pertaining to Russia's political agenda and influence operations (FireEye, 2017). The damages from APT28 include: (i) the breach of the Democratic Committees in 2016, that leaked thousands of politics-related files and caused the mistrust of the 2016 presidential electoral process (CrowdStrike, 2020); (ii) an attack against the World Anti-Doping Agency (WADA) in 2016, causing the private health information leak of Olympic athletes (Brady, 2018); and (iii) the compromise of corporate proprietary and individual private data from 2017 to 2021, where APT28 directed brute-force techniques against hundreds of government and private organizations (NSA, 2021).

Case Study: APT28 Attack Flows against U.S. Democratic Committees, 2016

In March 2016, APT28 targeted the Democratic Congressional Campaign Committee (DCCC) and the Democratic National Committee (DNC) to steal and expose data potentially damaging to the Clinton presidential campaign (Mueller, 2018). We observe three attack flows APT28 executed, which are highlighted in Figure 1 and detailed below.

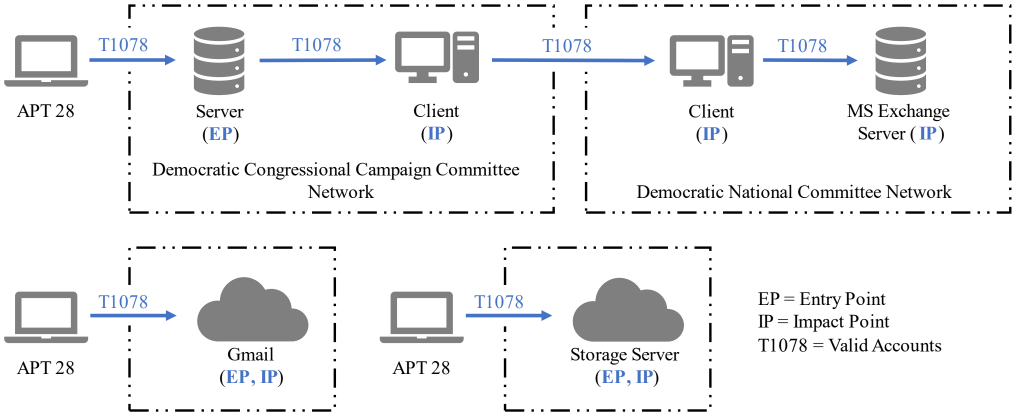

Figure 1: Three attack flows employed by APT28 against DCCC and DNC.

APT28 Attack Flow 1: Technical Description

In the first attack flow (Figure 1, top), the entry point for the attack was a public-facing server in the DCCC network. APT28 executed the Valid Accounts (T1078) attack technique to gain Initial Access into the DCCC network. To accomplish this, APT28 conducted Spearphishing with Links (T1598.003) that targeted DCCC employees with emails containing shortened URLs that resolved to attacker-controlled web servers, which replicated legitimate login portals. Consequently, APT28 obtained valid login credentials.

Then, APT28 Laterally Moved across the DCCC network by again employing Valid Accounts. It obtained the required credentials by deploying its XAgent malware on the victim systems to harvest credentials through Keylogging (T1056.001) and Exploitation for Credential Access (T1212). Likewise, APT28 Laterally Moved from the DCCC network into the DNC network, and across 33 DNC systems including an Exchange Server, with Valid Accounts (Mueller, 2018).

Finally, APT28 Exfiltrated over C2 Channels (T1041) with XAgent capturing sensitive files from the compromised systems. While few details were reported regarding C2 methods leveraged at the impact points shown in Figure 1, APT28 likely executed similar techniques as in other attacks, such as the attack against WADA, where C2 Web Protocols (T1071.001) like HTTP enabled the communication (Brady, 2018).

APT28 Attack Flow 2: Technical Description

In the second attack flow (Figure 1, bottom left), APT28 again leveraged Valid Accounts via Spearphishing with Links to gain access to a Clinton campaign chairman’s personal Gmail account. APT28 exfiltrated and subsequently leaked emails from this account. In this case, the entry point, attained through Valid

Accounts, and the impact point, sustained by Exfiltration Over Web Services (T1567), were both within the Gmail service.

APT28 Attack Flow 3: Technical Description

In the third attack flow (Figure 1, bottom right), APT28 again relied on Valid Accounts via Spearphishing with Links to gain access to a third-party cloud storage provider. APT28 Transferred Data to a Cloud Account (T1537) by abusing administrative functionality in the cloud management plane to create and exfiltrate snapshots of the victim servers to an attacker-owned account, which was registered with the same cloud service provider. In this case, the entry point and impact point were both within the third-party cloud storage server.

APT28 Attack Flows: Impact

The impact points of APT28 were the Exchange Server and client workstations in the DCCC and DNC networks, as well as the Gmail accounts and the third-party cloud storage server. Sensitive data, such as personal and professional correspondence, personally identifiable information (PII), and confidential data about the strategies and activities of the DCCC and DNC were compromised. APT28 exposed the pilfered data to damage the Clinton presidential campaign.

Strengths and Weaknesses of APT28

APT28’s strengths include developing malware with extensive capabilities as seen with XAgent, which has been continuously updated, showing that APT28 has evolved over time. XAgent’s extensiveness is evident in that it could compromise Windows, Linux, Mac, Apple, and Android operating systems (Axinte and Botezatu, 2017). Further, it could harvest credentials, install backdoors, evade defenses, scan networks, deploy keyloggers, capture victim screens, and exfiltrate data to C2 servers. The capabilities of XAgent enabled APT28 during multiple phases of its attacks while minimizing detection.

In terms of weaknesses, APT28 heavily relied on a few attack techniques, namely Valid Accounts and Spearphishing with Links. Consequently, if its social engineering campaigns were ineffective, then APT28 would not have gained initial access, lateral movement, privilege escalation, or exfiltration of sensitive data. APT28 also focused its resources on one variation of malware, namely XAgent. Throughout its attack against DCCC and DNC, APT28 uniformly relied on this malware, which proved effective. However, this makes defensive detection and response relatively easy. Had the victim organizations been more aware of XAgent, they could have uniformly disrupted the malware, and thus have thwarted APT28.

In-Depth Analysis of APT28

Analyzing APT28's Impact

From the financial impact perspective, we find APT28 does not appear financially motivated in the analyzed attack flows. In terms of data impact, APT28 was able to successfully expose sensitive documents related to political agendas. APT28's data impact also reveals its impact through publicity, as APT28 was credited with the disclosure of stolen data to manipulate public opinions in both DCCC and WADA campaigns (Brady, 2018; Mueller, 2018). In terms of operational impact, APT28 had relatively little focus on destructive techniques. This is reasonable because APTs, by definition, do not want to expose themselves by disrupting victims' routine operations because such disruptions would indicate the presence of attacks.

Analyzing APT28's Sophistication

In terms of attack flow difficulty, APT28's attack flows had little variance and required little technical knowledge to execute, despite that they did reflect some sophistication in coordinating multiple attack flows against different networks. From the perspective of attack novelty, APT28's ability to laterally move through multiple networks, cloud storage, and personal email accounts during the DCCC and DNC attack flows demonstrates APT28's advanced operational flexibility. Finally, in terms of resources employed, APT28 showed high sophistication through its various versions of XAgent malware, allowing for the use of XAgent in the majority of APT28's operations. Overall, APT28 is somewhat sophisticated. APT28's proprietary XAgent malware demonstrates significant engineering effort due to its many variations and modularity, indicating sophistication. However, APT28's reliance on Valid Accounts for Lateral Movement and Phishing for Initial Access indicates less sophistication since these methods are relatively easy to implement. This observation leads to an interesting insight into the minds of APT28. Although it possesses the capability to have a high level of sophistication, it is not against implementing relatively unsophisticated enabling procedures.

Insight 1. *APT28 exhibits the tendency to repeatedly use unsophisticated TTPs.*

Mitigation Approaches against APT28

In the case of APT28's attack flows against the Democratic Party, the root cause is social engineering, namely Spearphishing with Links. APT28's attack flows can thus be prevented with proper user training against phishing, antivirus solutions to detect malicious initial access files, web traffic filtering to prevent downloads of certain filetypes, and email filtering to perform message validation (Strom et al., 2018). Additionally, some elements of APT28's attack flows can be disrupted by general cybersecurity best practices, such as enforcing proper segmentation, vulnerability scanning, and behavior-based malware detection. For example, to prevent rampant usage of Valid Accounts, least privilege policies should be enforced with a secure multi-factor authentication implementation, which can be seen as one manifestation of zero-trust principles.

Insight 2. *The root cause of APT28's success tends to hinge on cyber social engineering attacks.*

Related Work

The importance of understanding offensive cyber operations has motivated many studies and efforts in industry, academia, and government. First, industry has proposed many frameworks, such as the Unified Kill Chain (Pols and Berg, 2017), Lockheed Martin's (2015) Cyber Kill Chain, and MITRE's ATT&CK framework (Strom et al., 2018). In addition, companies such as Mandiant, Microsoft, and CrowdStrike also provide CTI pertinent to APTs. The notion of cyberattack flow we propose goes further by holistically representing real-world cyber incidents.

Second, academic researchers have also proposed approaches to understand APTs (Tatam et al., 2021). These studies describe APT-style attacks from the perspective of threat frameworks, such as ATT&CK. However, they do not consider the *dynamics* or *temporal movement of attackers*, which is readily captured by the attack flow concept. This concept was inspired by the *cybersecurity dynamics* framework (Xu, 2014; Xu, 2019; Xu, 2020), which aims to mathematically model and analyze cybersecurity from a holistic perspective while explicitly considering the dynamics incurred by attack-defense interactions. The cybersecurity dynamics framework has led to many results in modeling attack-defense interactions (e.g., Han et al., 2021).

Third, the government, especially the Cybersecurity and Infrastructure Security Agency (CISA), also provides in-depth details of real-world APTs, often in the form of cybersecurity advisories, which summarize APTs' common TTPs, targets, and mitigations (e.g., CISA, 2020). However, they do not describe attack flows or analyze associated patterns, which are presented in this study.

Conclusion

This study presented a methodology of using attack flows to analyze APT attacks and demonstrated its usefulness in a case study on APT28. This led to a deepened understanding of APT28's strengths, weaknesses, impact, sophistication, and mitigations. However, more research is required to deeply understand the vast array of APTs. It would be beneficial to study the cybersecurity dynamics involved in closely related offensive cyber operations, such as those demonstrated in the real-world conflict between Russia and Ukraine. An initial study has been made towards understanding such all-domain operations (Ear et al., 2024b).

About the Authors

Logan Zeien is an undergraduate student pursuing his Bachelor of Science in Computer Science with an Emphasis on Cybersecurity at the University of Colorado, Colorado Springs (UCCS). He is a VICEROY Fellow. More information about Logan and his research can be found at https://linkedin.com/in/loganzeien/.

Caleb Chang is an undergraduate student pursuing a Bachelor of Science in Computer Science with an Emphasis on Cybersecurity at UCCS. He is a VICEROY Fellow and Caleb is also a winner of the 2024 USCYBERCOM CyberRecon Hunter Award. Find out more about Caleb at linkedin.com/in/caleb-c-chang/.

Lieutenant Colonel Ekzhin Ear is a U.S. Army Data Systems Engineer. He is currently pursuing a Ph.D. in Cybersecurity at UCCS while serving as a VICEROY mentor. Ekzhin is also a winner of the 2024 USCYBERCOM CyberRecon Hunter Award. Find out more about Ekzhin at https://linkedin.com/in/ekzhin-ear/.

Dr. Shouhuai Xu is the Gallogly Chair Professor in Cybersecurity, Department of Computer Science, UCCS. He is the PI and Director of the UCCS-led VICEROY Virtual Institute. His research has won several awards, including the 2019 Worldwide Adversarial Malware Classification Challenge organized by the MIT Lincoln Lab, the 2023 USCYBERCOM CyberRecon Analyst Award, and the 2024 USCYBERCOM CyberRecon Hunter Award. Find more information about his research at https://xu-lab.org.

Acknowledgement

This paper was supported in part by a VICEROY grant, a DoD UC2 grant, and Colorado State Bill 18-086. The opinions expressed in the paper are the authors' and do not necessarily reflect the view of the funding agencies or governments.

References

Axinte, Tiberius and Bogdan Botezatu (2017). *Dissecting the APT28 Mac OS X Payload*. Tech. rep. url: https://download.bitdefender.com/resources/files/News/CaseStudies/study/143/Bitdefender-Whitepaper-APT-Mac-A4-en-EN-web.pdf.

Brady, Scott (2018). *Indictment: United States of America vs. Aleksei Sergeyevich Morenets et. al.* url: https://nsarchive.gwu.edu/sites/default/files/documents /5513708/United-States-v-Alexei-Sergeyevich-Morenets-et.pdf.

CISA (2020). *North Korean Advanced Persistent Threat Focus: Kimsuky*. url: https://www.cisa.gov/news-events/cybersecurity-advisories/aa20301a.

CrowdStrike (2020). *CrowdStrike's work with the Democratic National Committee: Setting the record straight*. url: https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

CrowdStrike Intelligence (2022). *Early Bird Catches the Wormhole: Observations from the Stellar Particle Campaign*. url: https://www.crowdstrike.com/ blog/observations-from-the-stellarparticle-campaign/.

Ear, Ekzhin et al. (2023). “Characterizing Cyber Attacks against Space Systems with Missing Data: Framework and Case Study”. In: *2023 IEEE Conference on Communications and Network Security (CNS)*. IEEE, pp. 1–9. doi: 10.1109/ CNS59707.2023.10289045.

— (2024a). “Towards Principled Risk Scores for Space Cyber Risk Management”. In: arXiv preprint arXiv:2402.02635. url: https://arxiv.org/pdf/2402.02635.pdf.

— (2024b). “Characterizing Russia’s Cyber Operations in Ukraine through the Lenses of Cyber Attack Tactics, Techniques, and Procedures”. Manuscript under review by USCYBERCOM Cyber Recon’2024.

FireEye (2017). *APT28: At The Center of The Storm*. url: https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf.

Han, Yujuan et al. (2021). “Preventive and Reactive Cyber Defense Dynamics with Ergodic Time-dependent Parameters Is Globally Attractive”. In: *IEEE TNSE* 8.3, pp. 2517–2532.

Huntley, Shane (2022). *An update on the threat landscape*. url: https://blog.google/threat-analysis-group/update-threat-landscape-ukraine/.

Lockheed Martin (2015). *Gaining the Advantage: Applying Cyber Kill Chain Methodology to Network Defense*. url: https://www.lockheedmartin.com /content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advant age_Cyber_Kill_Chain.pdf (visited on 02/13/2024).

Mireles, Jose et al. (2016). “Extracting attack narratives from traffic datasets”. In: *2016 International Conference on Cyber Conflict, CyCon U.S. 2016, Washington, DC, USA, October 21-23, 2016*. Ed. by Aaron F. Brantly and Paul Maxwell. IEEE Computer Society, pp. 118–123.

Mueller, RS (2018). *Indictment: United States of America vs. Viktor Borisovich Netyksho et. al.* url: https://www.justice.gov/file/1080281/download.

NSA (2021). *Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments*. url: https://media.defense.gov/2021/Jul/01/2002753896/-1/-1/1/CSA_GRU_ GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF.

Pols, Paul and Jan van den Berg (2017). “The Unified Kill Chain”. In: *CSA Thesis, Hague*, pp. 1–104. url: https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain-Thesis.pdf.

Strom, Blake E et al. (2018). “Mitre att&ck: Design and philosophy”. In: *Technical report*. The MITRE Corporation. url: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf.

Tatam, Matt et al. (2021). “A review of threat modelling approaches for APT-style attacks”. In: *Heliyon* 7.1, pp. 1–19.

U.S. Army (2016). *Army Doctrine Reference Publication 3-0: Operations*. url: https://usacac.army.mil/sites/default/files/publications/ADRP%203-0%20OPERATIONS%2011NOV16.pdf.

UK Government (2021). *Russia: UK and US expose global campaign of malign activity by Russian intelligence services*. url: https://www.gov.uk/government/news/russia-uk-and-us-expose-global-campaigns-of-malign-activity-by-russian-intelligence-services.

Xu, Shouhuai (2014). “Cybersecurity Dynamics”. In: *Proc. Symposium on the Science of Security (HotSoS’14)*, 14:1–14:2.

— (2019). “Cybersecurity Dynamics: A Foundation for the Science of Cybersecurity”. In: *Proactive and Dynamic Network Defense*. Vol. 74. Springer.

— (2020). “The Cybersecurity Dynamics Way of Thinking and Landscape (invited paper)”. In: *ACM Workshop on Moving Target Defense*.