Effective Cyber Threat Hunting: Where and how does it fit?

Nombeko Ntingi, Petrus Duvenage, Jaco du Toit and Sebastian von Solms
Academy of Computer Science and Software Engineering, University of Johannesburg, South Africa
nntingi@gmail.com
duvenage@live.co.za
jacodt@uj.ac.za
basievs@uj.ac.za

Abstract: Traditionally threat detection in organisations is reactive through pre-defined and preconfigured rules that are embedded in automated tools such as firewalls, anti-virus software, security information and event management (SIEMs) and intrusion detection systems/intrusion prevention systems (IDS/IPS). As the fourth industrial revolution (4IR) brings with it an exponential increase in technological advances and global interconnectivity, the cyberspace presents security risks and threats the scale of which is unprecedented. These security risks and threats have the potential of exposing confidential information, damaging the reputation of credible organisations and/or inflicting harm. The regular occurrence and complexity of cyber intrusions makes the guarding enterprise and government networks a daunting task. Nation states and businesses need to be ingenious and consider innovative and proactive means of safeguarding their valuable assets. The growth of technological, physical and biological worlds necessitates the adoption of a proactive approach towards safeguarding cyber space. This paper centers on cyber threat hunting (CTH) as one such proactive and important measure that can be adopted. The paper has a central contention that effective CTH cannot be an autonomous 'plug in' or a standalone intervention. To be effective CTH has to be synergistically integrated with relevant existing fields and practices. Academic work on such conceptual integration of where CTH fits is scarce. Within the confines of the paper we do not attempt to integrate CTH with many of the various relevant fields and practices. Instead, we limit the scope to postulations on CTH's interface with two fields of central importance in cyber security, namely Cyber Counterintelligence (CCI) and Cyber Threat Monitoring and Analysis (CTMA). The paper's corresponding two primary objectives are to position CTH within the broader field of CCI and further contextualise CTH within the CTMA domain. The postulations we advanced are qualified as tentative, exploratory work to be expanded on. The paper concludes with observations on further research.

Keywords: cyber threat hunting, cyber counterintelligence, active cyber defense, cyber threat intelligence, cyber threat modelling, proactive

1. Introduction

Duvenage & von Solms (2013) rightly assert that the safeguarding of cyber space against emerging cyber threats does not only require the strengthening up of existing security measures, but also the introduction of proactive measures. Cyber threat hunting (CTH) is one such proactive and important measure that can be adopted.

The National Institute of Standards and Technology (NIST) defines CTH as a process to proactively identify and disrupt cyber threats inside the organisational ICT infrastructure and enhance security measures in order to defend against possible future threats (NIST, 2020). CTH is one of the more recently adopted methodologies implemented in the ICT sector. According to Lee & Lee (2017) the CTH field is relatively new and most security teams use unstructured methods of hunting. Lee & Lee (2017) further indicate that 45% of teams execute the threat hunting process on an *ad hoc* basis, with the main reason for this being the scarcity of published resources on structured hunting frameworks for adoption across the industry.

However, effective CTH cannot be an autonomous 'plug-in' or a standalone intervention. Its effectiveness can only be optimally leveraged when it is part of a broader cyber security approach. When it comes to finding postulations that integrate CTH with a broader cyber security approach, this is far easier said than done. In this regard, Kumar & Chacko (2020) states that while there are models, frameworks and systematic processes developed for CTH, much of the discussions published on these artefacts entail definitions and practical approaches to CTH activities *per se*. Kumar & Chacko (2020) further observes that there is a lack of propositions that integrate CTH as part of a broader approach. This observation confirms our literature review which likewise found a lack of such propositions.

This paper's first objective then is to introduce CTH and position it as an integral part of a broader CCI field. In addition to integration with a broader approach such as CCI, CTH is on a practical level dependent on close synergy with some of the elements of the Cyber Threat Monitoring and Analysis (CTMA) domain for its

effectiveness. The paper's second objective is thus to contextualise CTH as a critical dimension of the CTMA domain.

The rest of the paper is structured as follows: Section 2 positions CTH as an integral part of CCI with sub-section 2.1 defining the concept of CCI and its model and sub-section 2.2 contextualising CTH within the broader field of CCI. Section 3 introduces the CTMA domain, showing interrelation amongst the various aspects that enable effective CTH processes.

2. Positioning of cyber threat hunting within cyber counterintelligence (CCI)

In order to position CTH with CCI this section commences with a conceptual explication of CCI (Sub-section 2.1). Building on this explication, sub-section 2.2 positions CTH within the CCI context. Essentially then, this section seeks to answer the question: where and how does CTH fit in as far as CCI is concerned.

2.1 CCI: Concept and model

To provide a response to the question (where and how does CTH fit in as far as CCI is concerned?), this sub-section starts by defining and explaining CCI by means of a conceptual model. The various elements and modes/postures of the CCI model are discussed. The discussion in this sub-section will thus aid in accomplishing the paper's objective of positioning CTH into a broader context of CCI. According to Duvenage & von Solms (2014) CCI is part of a multi-disciplinary counterintelligence that aims to deter, prevent, degrade, exploit and neutralise attempts by adversaries that seek to alter confidentiality, integrity and availability of sensitive and critical information through methods of cyber.

Figure 1 below depicts a model for CCI as sourced from (Duvenage & von Solms, 2015). The figure shows four distinct quadrants (indicated by the four arrows) that represent CCI's four modes/postures namely: passive-defense, active-defense, passive-offensive and active-offensive. Positioned at the centre of the arrows is "IS" which denotes Intelligence and Strategy: CCI as a subset of counterintelligence thus puts business Intelligence and Strategy at the centre of operations in order to achieve business objectives (Duvenage & von Solms, 2015). The "CI" indicated on all four quadrants represents the multi-disciplinary field of Counterintelligence that relies on passive-active and defensive-offensive measures and means. CCI methods and means are indicated as part of the broader counterintelligence field.

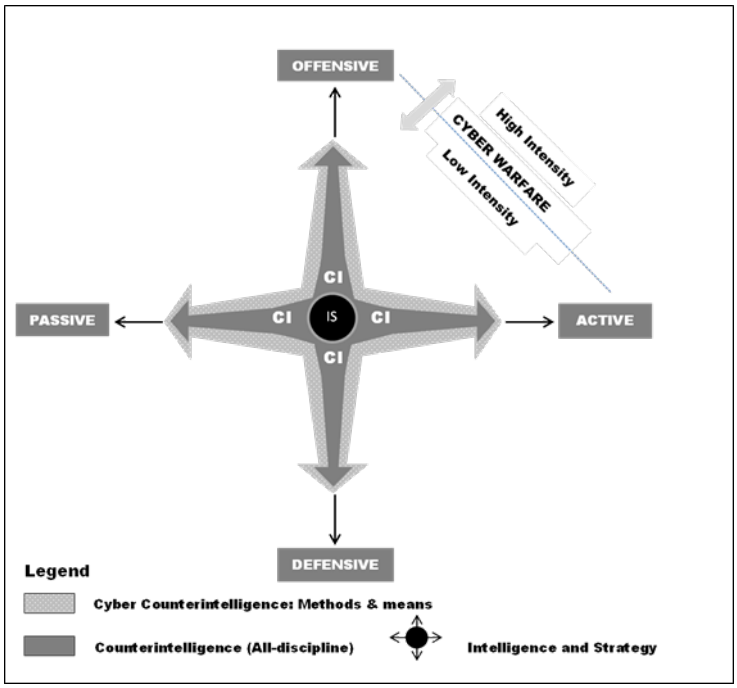

Figure 1: CCI model (Duvenage & von Solms, 2015)

According to Duvenage, Jaquire & von Solms (2016) defensive counterintelligence measures provide information and act as triggers to alert the offensive operations. Applied to this paper, the passive half of the CCI model (i.e. passive-defense and passive-offense quadrants) is deemed to incorporate the notion of 'information feeders'

and 'alerts'. 'Information feeders' and 'alerts' are thus in a symbiotic relationship with, yet distinctive from, active operations.

Furthermore, it has to be emphasised that *the deployment of the CCI model is context dependent*. With the realm of nation state counterespionage, Stech & Hechkman (2018) for example, concretised the CCI model with the following application to a hypothetical NATO operation against APT 28. Table 1 describes the application of the four-sector CCI matrix. It highlights the four quadrants as depicted in Figure 1. The columns describe the passive and active modes and the rows describe the defensive and offensive modes. The columns and rows depict the CCI tools and techniques for outsmarting the adversaries. Table 1 illustrates that defensive and offensive CCI tools can be deployed both passively and actively.

Table 1: Hypothetical NATO Cyber CI Operations against cyber espionage threat (Stech & Heckman, 2018)

Modes	Passive Cyber CI	Active Cyber CI
Defensive mode	**Deny access and collect on espionage threat**	
	Passive defense:	**Active defense:**
	Harden endpoint and server Configurations	Gather intelligence on on-going intrusions
		Use honeypots to gather late-stage implants and unpatched exploits
	Share actionable indicators across NATO intelligence partners	
		Share indicators to force infrastructure and "toolkit" rotations
Offensive Mode	**Manipulate, degrade, control and neutralise espionage threat**	
	Passive offensive:	**Active offensive:**
	Use honeypots to deliver deception materials	Counter-hack hop points and control servers
		Trolling "bait victims" to lure attackers to controlled boxes
	Sinkhole APT28 hop points	
	Identify APT28 operatives	Operating controlled boxes as double agents to inject beacons, double-hacked backdoors, etc. into APT28 control environment

While Table 1 applies the CCI matrix to the international state actor arena, it nonetheless conveys the essence of, and differences between, CCI's four quadrants more generally. With certain qualifications and changes, some of the techniques noted in Table 1 are therefore also useful to CCI and CTH as employed by non-state actors. Which of these techniques are relevant to CTH will depend on its (CTH's) positioning within CCI (See Subsection 2.2).

This sub-section defined and explained CCI by means of a conceptual model. As part of this explanation specific reference was made to the interface between the CCI model's active and passive modes. This interface is at the core of our postulation on the positioning of CTH as part of CCI in the next sub-section. The sub-section further illustrated the four-sector CCI matrix as applied in the NATO case study.

2.2 CTH in the context of CCI

This sub-section expounds CTH and conceptualise it within the context of CCI. A modified CCI model that depicts how CTH fits in with CCI will be presented. NIST released a special publication on September 2020 with CTH as an official cybersecurity discipline (Secureworks Counter Threat Unit, 2020). This means that organisations can incorporate CTH in their cyber security programs and collaborate on this with other organisations (Secureworks Counter Threat Unit, 2020). Sqrrl Data Inc (2016) describes CTH as an active means of defending ICT organisational infrastructure against adversaries by proactively and iteratively seeking unidentifiable or highly-obfuscated threats that lurk in organisational systems, networks and infrastructure. This is in contrast to the traditional means such as firewalls, intrusion detection and prevention systems, quarantining malicious code in sandboxes and SIEM technologies and systems which solely rely on pre-configured rules.

As mentioned in Section 1 of this paper, for the CTH approach to be effective, it needs to co-exist and be integrated in a wider discipline such as CCI. Figure 1 above provided a background of CCI and its means and methods as a subpart of a multi-disciplinary field.

Kolthoff (2015) suggests that cyber hunt team operations should be considered as a form of offensive counterintelligence even though they fall short of hacking back. Hacking back refers to organisations tracing back the origins of the cyber-attack and taking intrusive actions against the cyber-attackers (Kassner, 2021). According to Zimski (2021), hacking back is short-sighted and may have inadvertent repercussions. Instead the focus of any cyber security operation should always be to mitigate or neutralize the immediate threat (Herping, 2021). Furthermore, a cyber-operation carried out only for the goal of retaliation or punishment may increase the danger of escalation and may be illegal under international laws (Herping, 2021). Roberts (2020), asserts that in the cyber domain the lines between offensive and defensive operations are not always clear, mainly because offensive operations are being justified as defensive, moving acceptable standards toward the offensive end of the spectrum.

In our view, CTH in some respects not only forms part of CCI's active-defense mode, but also the active-offensive mode. We based our assertion on CTH's positioning on the explanation of the CCI model in subsection 2.1 as well as the foregoing narrative explanations of CCI and CTH. As will be explained per Figure 2, CTH is thus part of active CCI. With reference to Table 1, CTH would thus include techniques such as the use of honeypots to actively gather intelligence and the luring of attackers to controlled boxes.

In the interest of clarity, we concisely recapitulate our three main key contentions, namely

- To be effective CTH needs to be part of a broader approach such as CCI
- CTH is located with CCI's active modes (i.e. active-defense and active-offensive).
- While part of active CCI, CTH relies on functions provided by CCI's passive modes (i.e. passive-defense and passive-offense).

Figure 2 represents these contentions by means of a modified CCI model. Figure 2 shows CTH as located in CCI's active-defensive and active-offensive quadrants. Intelligence and Strategy (IS) is illustrated at the centre as the main objective to be delivered by the counterintelligence. The four quadrants depicted by the four arrows are all the counterintelligence postures. CCI as the subset of counterintelligence inherits the disciplines, methods and means of CI. CTH on its part serves as a compliment of the CCI multi-disciplinary field.

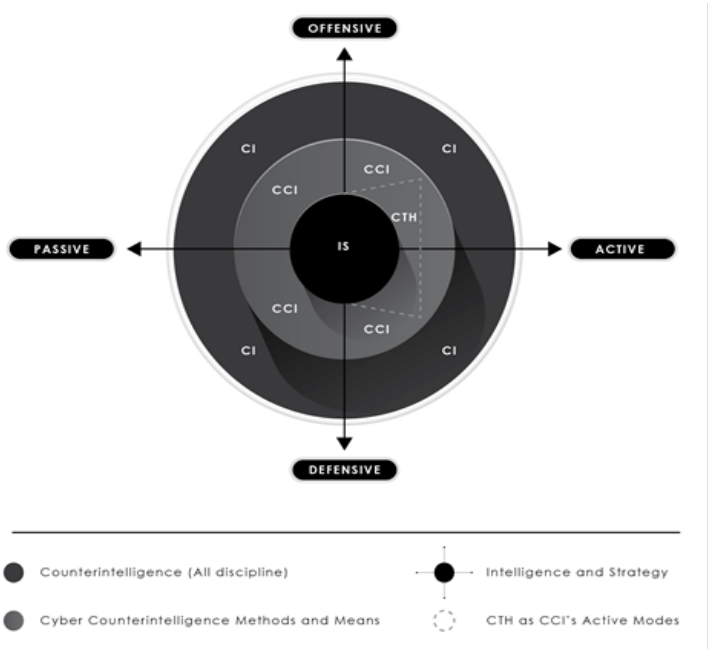

Figure 2: Cyber Threat hunting as part of cyber counterintelligence (Authors)

This section firstly focused on explaining the CCI concept and model as referenced from existing literature. CTH was then conceptualised and put in the context of CCI. A CCI model has been modified to illustrate where and how CTH fits in the four quadrants of the CCI model. Section 3 will introduce the CTMA domain and show how CTH can be contextualised within this domain. Section 3, more plainly put, will explore the question, where and how does CTH fit within the CTMA domain?

3. Introduction to the cyber threat monitoring and analysis (CTMA) domain

In this section the CTMA domain will be introduced along with some of its elements, as well as the interrelationships between these elements. This section will provide a brief background of the three CTMA domain elements in order to explain a close synergy of these elements. In order to illustrate the close synergy of the elements of the CTMA domain, this section will commence with illustrating CTMA domain in the CCI and locating the elements of the CTMA domain. The section will further explain the dependency of CTH processes to other elements of the CTMA domain. Subsections 3.2 and 3.3 will explicate CTI and CTM concepts in relation to CTH.

According to Singapore's Cyber Security Agency CSA (2021) cyber threat intelligence, cyber threat monitoring and cyber threat hunting are some of the elements of the wider CTMA domain, with CTI at the management level, CTM at the system level and CTH at an equipment or application level. Gumble (2020) states that CTM is a risk-based approach conducted to design secure systems with the purpose of identifying threats and designing mitigation strategies. According to RSI Security (2018) CTH and CTI are two of the most significant elements of cyber risk management since they enable organisations to adopt a proactive approach to hostile actors rather than reacting to issues as they arise.

As mentioned in Section 1, CTH is dependent on close synergy with some of the elements of CTMA domain for its effectiveness, Figure 3 (below) shows the location of these elements. According to CSA (2021) CTMA can be approached at three different tiers; namely management, system, equipment or application level perspectives. Prior to providing the graphic depiction (Figure 3), the elements of Figure 3 are narratively explained.

- **Management level:** The information/intelligence (cyber threat intelligence) gathered is used by Executive management for informed decision making. The intelligence gathered consist of actionable information to understand adversaries and their tactics, techniques and procedures (TTP). The purpose of data gathered is for the environmental scanning to gain understanding of the trends and cyber threats that the organisation is exposed to.
- **System level:** This level involves activities such as cyber threat modelling, it focuses on the system architecture, network and data visibility. At this level "Knowing your crown jewels" is critical, consequently data sources have to be identified. Crown jewels are critical assets to attaining the overall corporate objectives, and they are typically the targets of attackers. The crown jewels and privileged accounts need to be properly identified for purposes of data modelling.
- **Equipment or application level:** This level involves the more technical activities such as CTH activities, cyber security event logs and analytics. From Figure 3, CTH is demonstrated as a low-level activity that focusses on technical perspectives. The focus of the paper at the moment is limited to CTH. It is for this reason the "equipment or application level" in Figure 3 is highlighted with a different shade.

Figure 3: Elements of the CTMA domain (CSA 2021)

Figure 3 above shows the interrelationship between some of the elements of the CTMA domain. Figure 4 will now magnify Figure 3 to further illustrate how CTMA domain as a whole fit into CCI and specifically where CTH is located within the CTMA domain. Figure 4 is an adaptation of Figure 2, for simplicity the graphic depiction of Figure 4 only shows the CCI means and methods as the four quadrants represented by the arrows. The triangle displayed on its side is adopted from Figure 3 to show how the elements of the CTMA domain fit into the CCI

model. The CTMA domain, which includes the CTI, CTM and CTH spans across all four quadrants to demonstrate that CTMA as a whole is executed in all the four quadrants of CCI. CTH is represented at the lower level of the CTMA domain in the active quadrants of CCI, namely (active-defensive and active-offensive). Our key contention is that CTMA is performed in all four quadrants of CCI and that CTH is located in the two active quadrants of CCI.

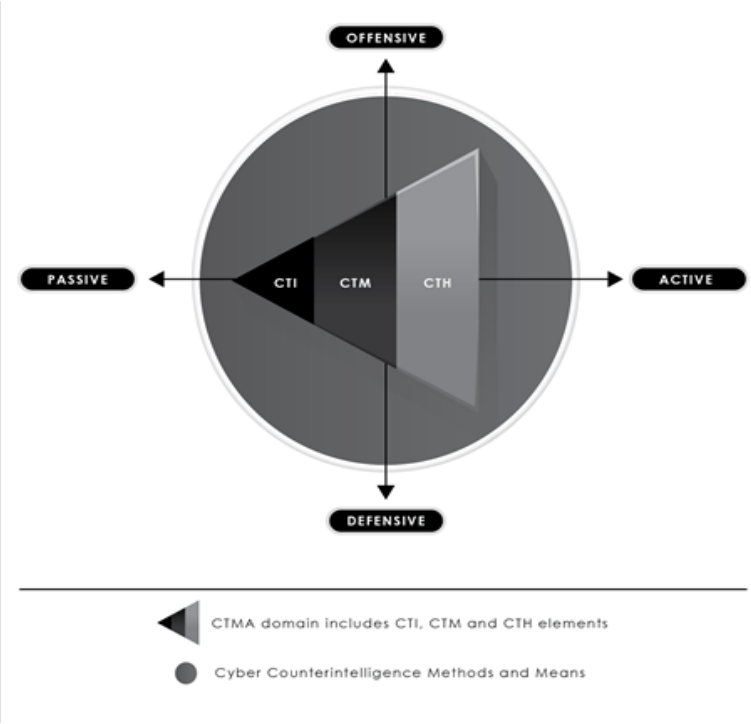

Figure 4: CTMA domain as located in the four quadrants of CCI (authors)

Figure 3 showed the interrelationship between these elements, with CTH located at the lower level of the hierarchy where the technical activities occur. According to IBM (2021) success and effectiveness of CTH depends on the accuracy and abundance of data gathered. Sapphire (2021) states that CTH leverages intelligence collected and processed during CTI process. That is to say CTI acts as an information feeder for CTH processes. Cyber threat hunters also rely on access to both host and network data sources identified during CTM to conduct hypotheses investigations, (ChaosSearch, 2021).

This section illustrated the interrelationships between the CTMA domain's elements, as well as where the CTMA domain as a whole fits within the CCI discipline's four quadrants. CTH was also shown to be in the active quadrants of the CCI model. Building on the foregoing positioning of CTMA domain in the CCI discipline and CTH as part of the CTMA domain, the next sub-sections explain in more detail CTH's relation with CTI and CTM respectively and how they contribute to the success of CTH processes.

3.1 The concept of CTI and its relation to CTH

Baker (2021) defines CTI as information that is processed, evaluated and driven by evidence about existing or emerging threats to organisational assets. This evidence-based knowledge is useful during decision making. The aim of CTI is to scan and understand the environment within which the organisations or nation states operate in. This environmental scanning helps the organisations to understand who their adversaries/competitors are and why are they being targeted. In Section 1 it was mentioned that there are dependencies for CTH processes to occur. Puzis et al (2020) states that for CTH to effectively conduct its processes such as hypotheses formulation, it relies on clear-cut evidence collected and analysed during the CTI process. Evidence based data collected during the CTI process which lies in the management level of the CTMA domain aids in making informed decisions by the executive management and serve as input to perform the CTH processes. The effectiveness of CTH processes depend on the ability of accurate collection and analysis of data.

Following explanation of CTH's relationship with CTI, we now proceed with examining the concept of CTM and how it relates to CTH.

3.2 The concept of CTM and its relation to CTH

Kost (2021) defines CTM as a proactive approach in which organisations identify potential and anticipated threats in their network security and the vulnerabilities that can be exploited by these threats. CTM can be used to prevent cyber threats from taking advantage of the system flaws by using threat modelling methods to inform defensive measures. CTM focuses on system architecture, relationships and behaviours as well as data sources such as endpoint information, logs from firewalls, and domain name services. CTH is a data driven process hence data and network visibility is of utmost importance. As mentioned in section 3, CTM which is at system level focusses on network and data visibility. According to ChaosSearch (2021), cyber threat hunters must have access to data sources that provide visibility into host and network activity, as well as telemetry data obtained by security solutions currently in use in the environment.

This section firstly introduced the CTMA domain and how the elements of CTMA relate. The interrelationships of CTI and CTM with CTH were further described in sub-sections 3.1 and 3.2, respectively. Section 3 attempted to answer the question, "Where and how does CTH fit within the CTMA domain?"

4. Conclusion

For the organisations to be more effective in defending their ICT infrastructure from an ever-expanding cyber threat base, a shift towards proactive techniques to improve their security posture should be at the forefront.

This paper explored CTH as one of the more recent such proactive methodologies. The paper highlighted the need for academic research to integrate CTH with relevant, existing fields and practices. Phrased differently, for CTH to be effective we need to be clear on where and how it fits with existing fields and practices. We thus proceeded with postulations on CTH's interface with two fields of central importance in cyber security, namely CCI and CTM. These should be viewed as tentative propositions and form part of the quest for an academic foundation for developing an active cybersecurity posture for organisations and nation-states exposed to increasingly sophisticated attacks. An integration of cyber threat hunting into other disciplines will provide a solid foundation and develop a cyber-defense active environment for organisations to expose sophisticated attack mechanisms and test their ability to detect attacks thus enabling organisations and nation states to become effective in the quest of active cyber defense activities.

References

Baker, K. 2021. What is Cyber Threat Intelligence. [Online] Available at: https://www.crowdstrike.com-/cybersecurity-101/threat-intelligence/ [Accessed 27 12 2021].

CSA Singapore 2021. A Singapore Government Agency Website. [Online] Available at: https://www.csa.gov.sg/-/media/csa/documents/legislation_supplementary_references/guide-to-cyber-threat-modelling.pdf [Accessed 08 11 2021].

ChaosSearch, 2021. The Threat Hunter's Handbook. [Online] Available at: https://www.chaossearch.io/hubfs-/ChaosSearch%20Threat%20Hunters%20Handbook.pdf [Accessed 08 02 2022].

Duvenage, P, Jaquire, V & von Solms, S. 2016. 'Conceptualising cyber counterintelligence – Two tentative building blocks' in Published Proceedings of the 15th European Conference on Cyber Warfare and Security, Munich, Germany, June.

Duvenage, P. & von Solms, S. 2013. The Case for Cyber Counterintelligence. Pretoria, IEEE.

Duvenage, P. & von Solms, S. 2014. Putting Counterintelligence in Cyber Counterintelligence. Greece, Academic Conferences and Publishing International Limited.

Duvenage, P. & von Solms, S. 2015. Cyber Counterintelligence: Back to the Future. Journal of Information Warfare, 13(4), pp. 42-56.

Gumbley, J., 2020. A Guide to Threat Modelling for Developers. [Online] Available at: https://martinfowler.com/articles/agile-threat-modelling.html [Accessed 03 02 2022].

Herping, S., 2021. Active Cyber Defense Operations. [Online] Available at: https://www.stiftung-nv.de/sites/default/files/active_cyber_defense_operations.pdf [Accessed 18 03 2022].

IBM, 2021. Cyber Threat Hunting. [Online] Available at: https://www.crowdstrike.com/cybersecurity-101/threat-hunting/ [Accessed 01 02 2022].

Kassner, M. 2021. Is hacking back affective, or does it just scratch an evolutionary itch? [Online] Available at: https://www.techrepublic.com/article/is-hacking-back-effective-or-does-it-just-scratch-an-evolutionary-itch/ [Accessed 27 12 2021].

Kolthoff, J. 2015. https://www.linkedin.com. [Online] Available at: https://www.linkedin.com/pulse/cyber-counterintelligence-hunt-team-operations-jarrett-kolthoff/ [Accessed 08 11 2021].

Kost, E. 2021. What is threat modelling. [Online] Available at: https://www.upguard.com/blog/what-is-threat-modelling [Accessed 27 12 2021].

Kumar, A. & Chacko, A. 2020. Security Intelligence. [Online] Available at: https://securityintelligence.com/posts/threat-hunting-guide/ [Accessed 12 11 2021].

Lee, R. & Lee, R. M. 2017. The Hunter Strikes Back: The SANS 2017 Threat Hunting Survey. [Online] Available at: https://www.malwarebytes.com/pdf/white-papers/sans_report-the_hunter_strikes_back_2017.pdf [Accessed 12 10 2021].

National Institute of Standards and Technology, 2020. Security and Privacy Controls for Information Systems and Organisations, Washington, D.C.: s.n. [Accessed 12 10 2021].

Puzis, R., Zilberman, P. & Elovici, Y., 2020. [Online] Available at: https://www.researchgate.net/publication-/339814086_ATHAFI_Agile_Threat_Hunting_And_Forensic_Investigation [Accessed 07 01 2022].

Roberts, M., 2020. The Cyber-Range Advantage for Defence. [Online] Available at: http://www.milsatmagazine.com/story.php?number=1777803179&msclkid=b6514886a67511ec9524dd5dd0476196 [Accessed 18 03 2022].

RSI Security, 2018. Understanding the basic components of cyber risk management. [Online] Available at: https://blog.rsisecurity.com/understanding-the-basic-components-of-cyber-risk-management/[Accessed 07 02 2022].

Secureworks Counter Threat Unit 2020. Research & Intelligence. [Online] Available at: https://www.secureworks.com/blog/threat-hunting-as-an-official-cybersecurity-discipline [Accessed 30 12 2021].

Sqrrl Data Inc 2016. A Framework for Cyber Threat Hunting. [Online] Available at: https://www.threathunting.net/files/framework-for-threat-hunting-whitepaper.pdf

Stech FJ & Heckman KE 2018 'Human nature and cyber weaponry: Use of denial and deception in cyber counterintelligence', Cyber Weaponry Issues and Implications of Digital Arms, H Prunckun (ed), Springer, Cham, CH.

Zimski, P., 2021. Why companies should never hack back. [Online] Available at: https://www.helpnetsecurity.com/2021/08/31/why-companies-should-never-hack-back/?web_view=true [Accessed 18 03 2022].