Journal of Information Warfare

Volume 19, Issue 1
2020

Contents

A Cyber Counterintelligence Matrix for Outsmarting Your Adversaries

PC Duvenage, VJ Jaquire, and SH von Solms

Centre for Cyber Security
Academy of Computer Science and Software Engineering
University of Johannesburg, South Africa

E-mail: duvenage@live.co.za; jaquire@gmail.com; basievs@uj.ac.za

Abstract: *While Cyber CounterIntelligence (CCI) has been a distinctive specialisation field for state security structures internationally for well over a decade, recently there has been growing recognition of CCI's significance to non-state actors. CCI is central to proactively mitigating cyber risk and exploiting opportunities. With the growing recognition of CCI's significance comes an appreciation of its complexity. CCI is all about out-thinking and outwitting adversaries. This article advances a conceptual matrix that can serve both as a high-level 'pocket guide' for outsmarting adversaries and as an aid to academic research.*

Keywords: *Cyber Security, Cyber Counterintelligence, Risk Management, Offensive Cybersecurity, Threat Intelligence, Information Warfare, Information Operations*

Introduction

Nation states and non-state organisations are increasingly targeted not only by adversarial state actors, but also by other classes of actors with significant intelligence capacities, such as crime syndicates, competitors, and some corporate entities (Coats 2018; Symantec 2018). Concomitantly, there has been a sharp increase in the number and the scale of state and non-state actors' utilisation of cyber space for intelligence gathering. In 2018, the number of "Targeted Attack Groups" tracked by Symantec, for example, stood at 155, a staggering 78% increase from the 87 groups monitored in 2015 (Symantec 2018, 2019). According to Symantec (2019) 'intelligence gathering' was a primary motive for 96 % of attacks by these groups during 2018. As is clear from **Figure 1**, intelligence gathering dwarfs other known attack motives.

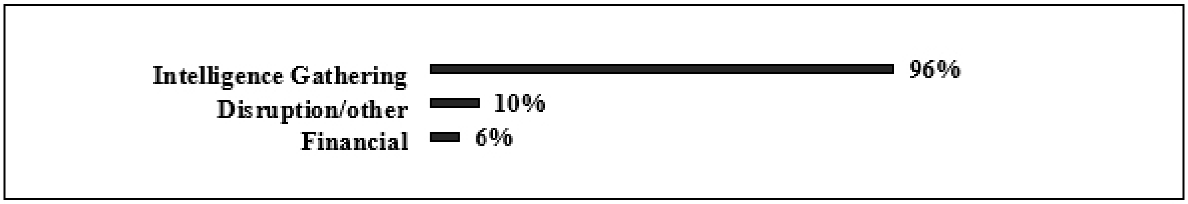


Figure 1: Targeted attack groups: Known attack motives (Symantec 2019)

The countering of adversarial intelligence gathering through cyber means is cyber counterintelligence's signature role. While cyber counterintelligence (CCI) has been a distinctive specialisation field for state security structures internationally for well over a decade, there is now growing recognition of CCI's significance also to non-state actors. CCI is gaining main stream traction and is seen as central to proactively mitigating cyber risk and exploiting opportunities. The cybersecurity vendor Panda Security (2018:1), for example, recently observed that CCI has increasingly become "more significant among larger companies". Also, for smaller role players lacking the resources for a fully-fledged capacity, CCI offers a way of thinking and an approach towards more robustly asserting their cyber interests (Jaquire, Duvenage & von Solms 2018).

With the growing recognition of CCI's significance comes an acknowledgment of its complexity. CCI is not an easy-to-use add-on or plug-in. It is all about the meticulous out-thinking and outwitting of actual and potential adversaries. This article advances a matrix that can serve as a concise, high-level 'pocket guide' for outsmarting adversaries through a robust CCI effort. Premised on CCI's passive-defensive and active-offensive dimensions, the matrix (1) guides the optimal deployment of offensive and defensive tools and techniques; (2) synchronises and integrates CCI with organisational processes; and (3) aids the configuration of a CCI posture best suited for organisations' varying requirements.

The remainder of this article consists of five parts:

- A cursory overview of the CCI matrix and its two composite parts (namely a vertical plane and a horizontal plane);
- A description of the CCI matrix's horizontal plane which explains CCI's passive-active and defensive-offensive modes;
- A discussion of the CCI matrix's vertical plane by explaining the different levels of CCI's execution—namely strategic, operational, and tactical-technical;
- A case study illustrating the CCI matrix's application;
- The authors' conclusions.

Overview of the CCI Matrix

The CCI matrix advanced in this article is a three-dimensional concept comprising a vertical and horizontal plane, which is graphically presented in **Figure 2**, below:

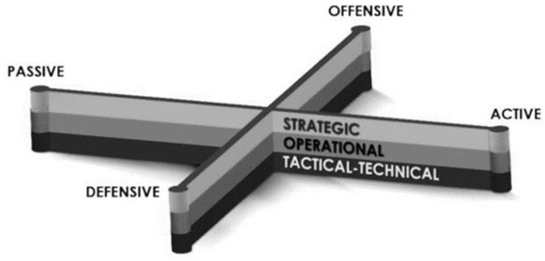


Figure 2: The cyber counterintelligence matrix

The CCI matrix's horizontal plane depicted in **Figure 2** represents the four quadrants of the CCI posture, namely

- Passive-defensive
- Active-defensive
- Active-offensive
- Passive-offensive

The CCI matrix's vertical plane aligns CCI with broader organisational processes (such as counter-intelligence—CI) at the three organisational levels/layers on which CCI operates, namely

- Strategic
- Operational
- Tactical/Technical

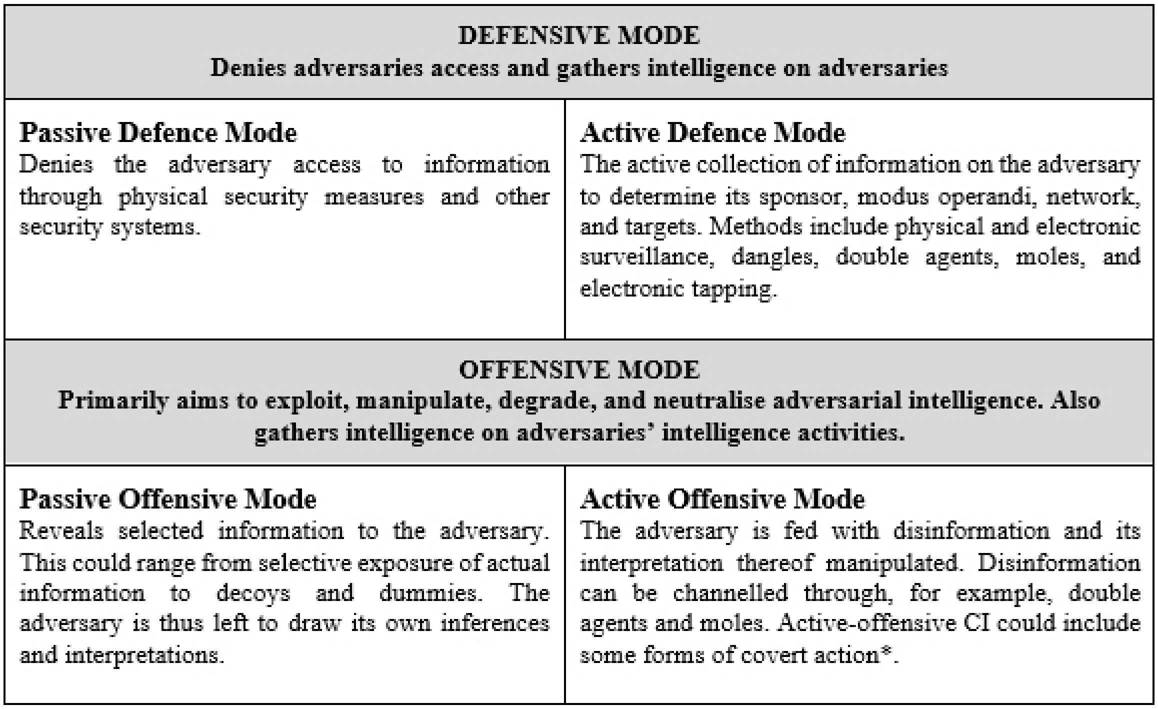
This section briefly outlined the CCI matrix's composition. The next section explains the CCI matrix's horizontal plane.

Horizontal Plane of the Matrix: The Cyber Counterintelligence Modes

As noted in this article's introduction, CCI is not an easy-to-use add-on or plug-in. To be effective, CCI needs to be executed as part of an organisation's counterintelligence (CI) efforts. Because it is a CI subset, CCI is underpinned by time-tested CI principles, notions, and concepts.

Counterintelligence fundamentals underpinning the CCI matrix

The CCI matrix's horizontal plane is premised on two fundamental CI notions. First, for a significant part, the wide array of CI tools and techniques can be used for both defensive and offensive purposes. Secondly, both offensive and defensive tools can be deployed passively and/ or actively. Flowing from these two assertions, the authors infer four modes for deploying CI tools and techniques, namely passive-defensive, active-defensive, passive-offensive, and active-offensive. Within CI generally, these modes can be summarised in tabulated format in **Figure 3**, below, which was adapted from Duvenage and von Solms (2013), as compiled from narratives in Prunckun (2012) and Sims (2009).



<table>
<tr><th colspan="2">DEFENSIVE MODE
Denies adversaries access and gathers intelligence on adversaries</th></tr>
<tr><td><b>Passive Defence Mode</b>
Denies the adversary access to information through physical security measures and other security systems.</td><td><b>Active Defence Mode</b>
The active collection of information on the adversary to determine its sponsor, modus operandi, network, and targets. Methods include physical and electronic surveillance, dangles, double agents, moles, and electronic tapping.</td></tr>
<tr><th colspan="2">OFFENSIVE MODE
Primarily aims to exploit, manipulate, degrade, and neutralise adversarial intelligence. Also gathers intelligence on adversaries’ intelligence activities.</th></tr>
<tr><td><b>Passive Offensive Mode</b>
Reveals selected information to the adversary. This could range from selective exposure of actual information to decoys and dummies. The adversary is thus left to draw its own inferences and interpretations.</td><td><b>Active Offensive Mode</b>
The adversary is fed with disinformation and its interpretation thereof manipulated. Disinformation can be channelled through, for example, double agents and moles. Active-offensive CI could include some forms of covert action*.</td></tr>
</table>

Figure 3: Four-sector counterintelligence matrix (adapted from Duvenage & von Solms 2013; Prunckun 2012; Sims 2009)

*Covert action, in the context of its use in **Figure 3**, denotes the targeting of an adversary through the influencing of events, conditions, individuals, groups, or institutions to the benefit of a sponsor in a manner not attributable to the sponsor or offering plausible deniability. Influencing is achieved through measures that vary from paramilitary and political actions to propaganda and intelligence assistance.

Application of the four sector CI matrix to CCI

The four-sector CI matrix is applicable to the full spectrum of CCI tools and techniques. At the one end of the spectrum, conventional Intrusion Prevention Systems (IPS)/Intrusion Detection Systems (IDS) serve as examples of passive-defensive tools. At the other end of the spectrum, a cyber weapon designed to destroy, disrupt, or manipulate an opponent’s systems constitutes an active-offensive tool. CCI tools and techniques can seldom be pigeonholed as having only a defensive or offensive purpose, or as being either active or passive. It must be emphasised that, for the most part, tools and techniques are useful to two or more of the four modes. A honeynet, for example, can be used passive-offensively (for example, to feed disinformation to an adversary) and active-defensively (such as to collect information on an opponent). The multiple uses of CCI tools are discussed comprehensively in earlier research (Jaquire 2018; Duvenage 2019). For purposes of this article, only a small selection of these tools and techniques are plotted in **Figure 4**, below.

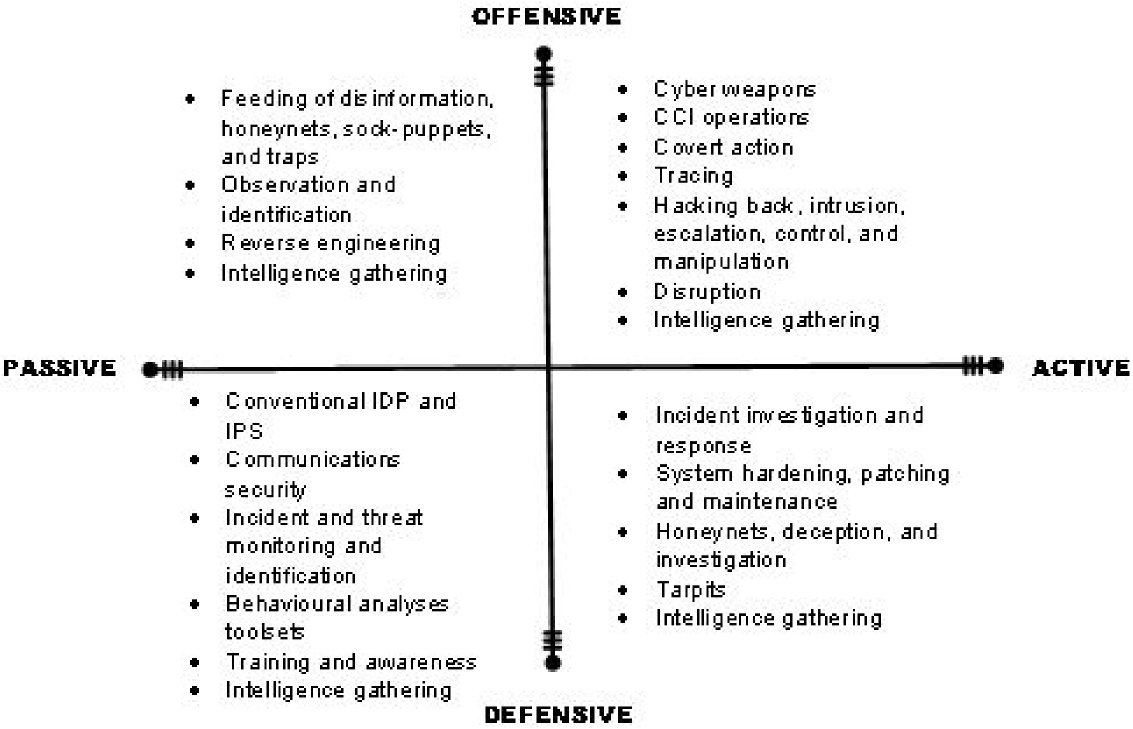

OFFENSIVE
Feeding of disinformation, honeynets, sock-puppets, and traps
Observation and identification
Reverse engineering
Intelligence gathering
Cyber weapons
CCI operations
Covert action
Tracing
Hacking back, intrusion, escalation, control, and manipulation
Disruption
Intelligence gathering
PASSIVE
ACTIVE
Conventional IDP and IPS
Communications security
Incident and threat monitoring and identification
Behavioural analyses toolsets
Training and awareness
Intelligence gathering
Incident investigation and response
System hardening, patching and maintenance
Honeynets, deception, and investigation
Tarpits
Intelligence gathering
DEFENSIVE

Figure 4: A variety of CCI tools and techniques plotted on the CCI Matrix's horizontal plane

As an academic construct, **Figure 4** is useful to categorise CCI tools and techniques and to explain their relationship with other non-cyber CI tools and techniques.

In CCI practice, **Figure 4** could have the following three uses:

1) Ensure each CCI tool is utilised to maximum effect. Since most tools and techniques can have more than one purpose, they should be measured against the CCI matrix with the following question: 'In addition to its initially intended role, in what other modes can the tool or technique be used?'. **Figure 4**, above, for example, depicts a honeynet deployed in both the active-defensive and passive-offensive modes. A honeynet can also, if required, be used to facilitate hacking back and deploying cyber weapons (active-offensive). If otherwise configured, a honeynet could also be deployed in tandem with IDS/IPS (passive-defensive). In this hypothetical example, a honeynet is therefore relevant to all four modes.
2) Synchronise CCI tools/techniques with other CI tools/techniques. The plotting of CCI and other CI tools/actions in **Figure 4**, above, aids the synchronisation of efforts and thus optimises the effectiveness and integration of CCI with the overarching CI effort. In addition to CCI, the broader CI effort includes Human Intelligence (HUMINT) and additional non-cyber technical means. The synergy required between CCI and broader CI can be explained more practically by means, on one hand, of a conventional human double agent, and on the other hand, of a cyber honeynet and sock puppet. The feeding of disinformation through a human double agent should be congruent with disinformation planted in an organisation's honeynet and its sock puppets' 'actions'. Inconsistencies between these feeds of disinformation could compromise both CI human operations and CCI

operations. The opposite is also true—synchronising CI human operations and CCI actions maximises effect and impact.

3) Configure the CCI posture in accordance with the type and needs of a specific organisation. The matrix in **Figure 4**, above, can aid in configuring a CCI posture that is best suited for an organisation's varying requirements. In this illustration, a comparison is made between the CCI posture of a nation state and that of a health care provider. A nation state and health care provider will both allocate substantial resources to the passive-defence quadrant. However, a nation state will also typically devote significantly more resources to the three other quadrants. It is important to note that a health care provider should devote at least some resources to quadrants other than the passive defensive. The degree and nature to which a health care provider would engage in the offensive quadrants will, of course, be determined by numerous factors which include legal considerations and cooperation with state authorities on specific offensive actions.

Figure 5, below, depicts the preceding narrative comparison of a nation state's and a health care provider's respective CCI postures.

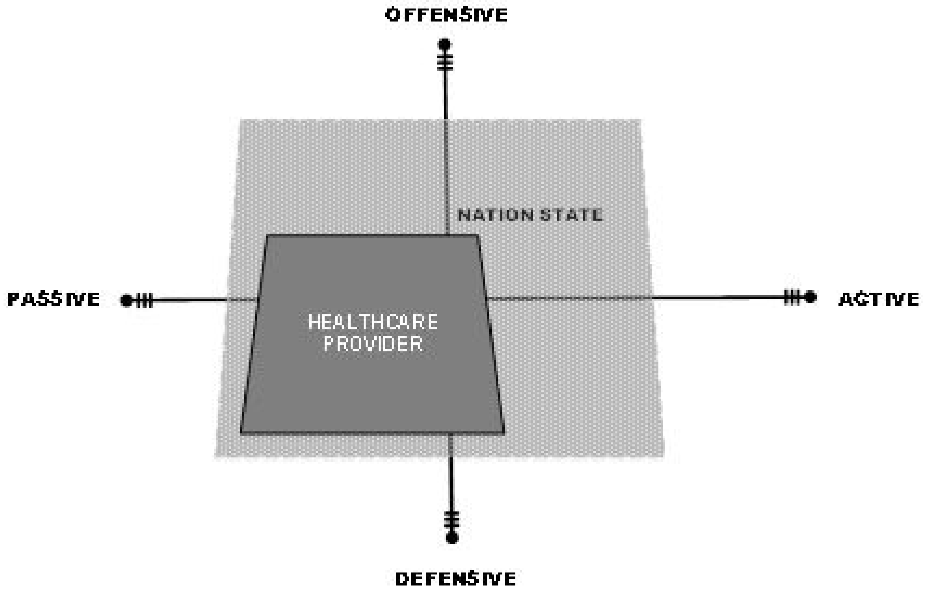
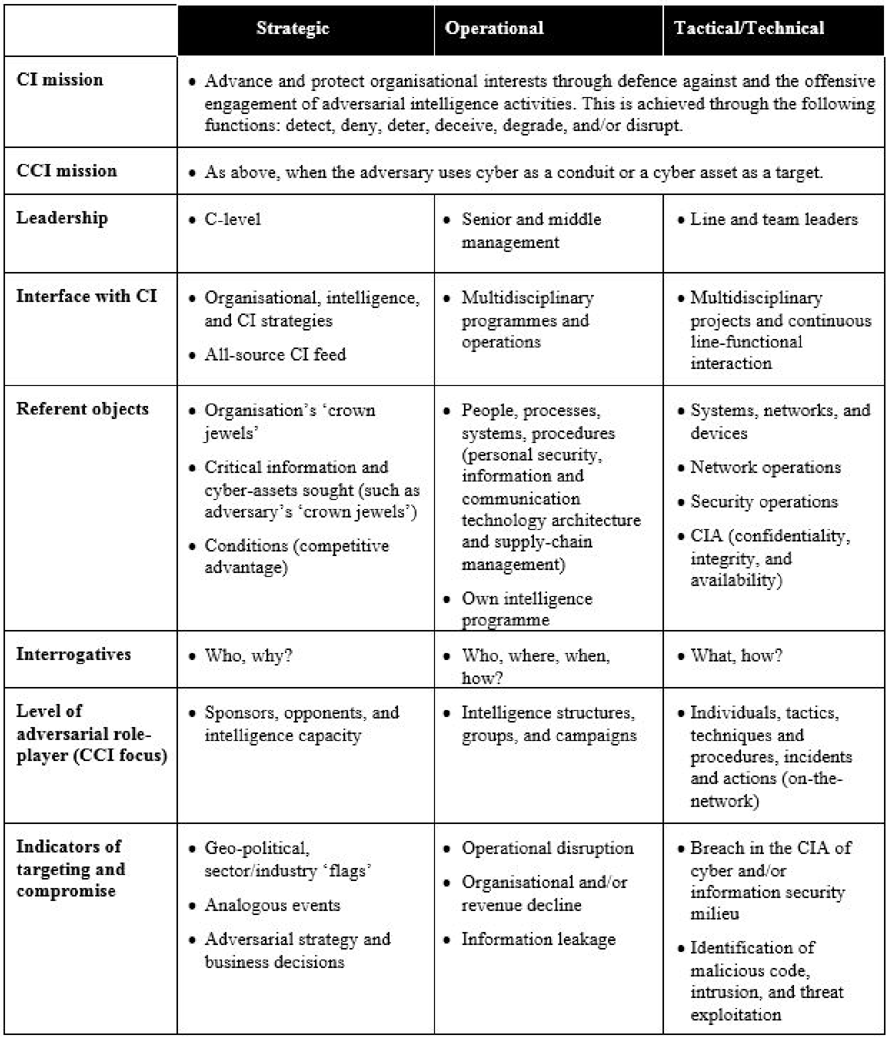


Figure 5: Juxtaposing CCI postures of a nation-state security structure and a health care provider

The degree and nature to which a health care provider would engage in the offensive quadrants will of course be determined by numerous factors, which include legal considerations and cooperation with state authorities on specific offensive actions. This comparison is illustrated in **Figure 5**, above. Implicit in this comparison is the notion that the configuration of the organisation's CCI posture on the strategic levels (interests, goals, and strategy) will ultimately shape CCI activities on the operational and tactical-technical level. These different levels are discussed in the next section as the CCI matrix's horizontal plane.

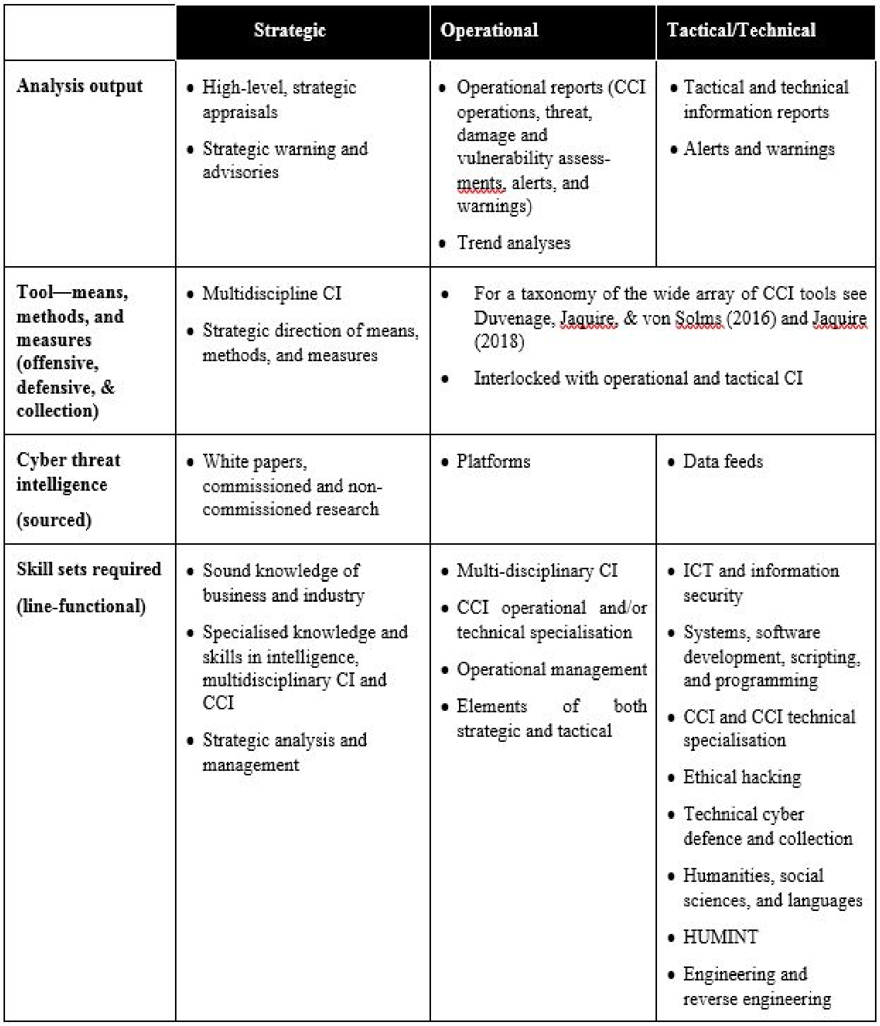
Vertical Plane of the CCI Matrix: Levels of Execution

The CCI matrix's vertical plane explains the various levels on which CCI functions and integrates CCI with the broader organisational postures and processes. Since CCI is a CI subset, the importance of synchronising and integrating CCI with the organisational CI endeavour on all levels cannot be overemphasised. As was the case with the development of the horizontal plane, the design of the vertical plane is based on a well-established CI notion, namely the three levels of execution (strategic, operational, and tactical). These levels and their interplay have been described in more detail in existing research, including van Niekerk and Duvenage (2016); Duvenage, Jaquire, and von Solms (2016); Stech and Heckman (2018); and Jaquire (2018). The authors developed the synopsis shown in **Figure 6**, below.



	Strategic	Operational	Tactical/Technical
CI mission	• Advance and protect organisational interests through defence against and the offensive engagement of adversarial intelligence activities. This is achieved through the following functions: detect, deny, deter, deceive, degrade, and/or disrupt.		
CCI mission	• As above, when the adversary uses cyber as a conduit or a cyber asset as a target.		
Leadership	• C-level	• Senior and middle management	• Line and team leaders
Interface with CI	• Organisational, intelligence, and CI strategies • All-source CI feed	• Multidisciplinary programmes and operations	• Multidisciplinary projects and continuous line-functional interaction
Referent objects	• Organisation's 'crown jewels' • Critical information and cyber-assets sought (such as adversary's 'crown jewels') • Conditions (competitive advantage)	• People, processes, systems, procedures (personal security, information and communication technology architecture and supply-chain management) • Own intelligence programme	• Systems, networks, and devices • Network operations • Security operations • CIA (confidentiality, integrity, and availability)
Interrogatives	• Who, why?	• Who, where, when, how?	• What, how?
Level of adversarial role-player (CCI focus)	• Sponsors, opponents, and intelligence capacity	• Intelligence structures, groups, and campaigns	• Individuals, tactics, techniques and procedures, incidents and actions (on-the-network)
Indicators of targeting and compromise	• Geo-political, sector/industry 'flags' • Analogous events • Adversarial strategy and business decisions	• Operational disruption • Organisational and/or revenue decline • Information leakage	• Breach in the CIA of cyber and/or information security milieu • Identification of malicious code, intrusion, and threat exploitation

Figure 6: Synopsis of the levels of CCI execution (adapted from Duvenage, Jaquire & von Solms 2016)



	Strategic	Operational	Tactical/Technical
Analysis output	• High-level, strategic appraisals • Strategic warning and advisories	• Operational reports (CCI operations, threat, damage and vulnerability assess-ments, alerts, and warnings) • Trend analyses	• Tactical and technical information reports • Alerts and warnings
Tool—means, methods, and measures (offensive, defensive, & collection)	• Multidiscipline CI • Strategic direction of means, methods, and measures	• For a taxonomy of the wide array of CCI tools see Duvenage, Jaquire, & von Solms (2016) and Jaquire (2018) • Interlocked with operational and tactical CI	
Cyber threat intelligence **(sourced)**	• White papers, commissioned and non-commissioned research	• Platforms	• Data feeds
Skill sets required **(line-functional)**	• Sound knowledge of business and industry • Specialised knowledge and skills in intelligence, multidisciplinary CI and CCI • Strategic analysis and management	• Multi-disciplinary CI • CCI operational and/or technical specialisation • Operational management • Elements of both strategic and tactical	• ICT and information security • Systems, software development, scripting, and programming • CCI and CCI technical specialisation • Ethical hacking • Technical cyber defence and collection • Humanities, social sciences, and languages • HUMINT • Engineering and reverse engineering

Figure 6, cont'd**:** Synopsis of the levels of CCI execution (adapted from Duvenage, Jaquire & von Solms 2016)

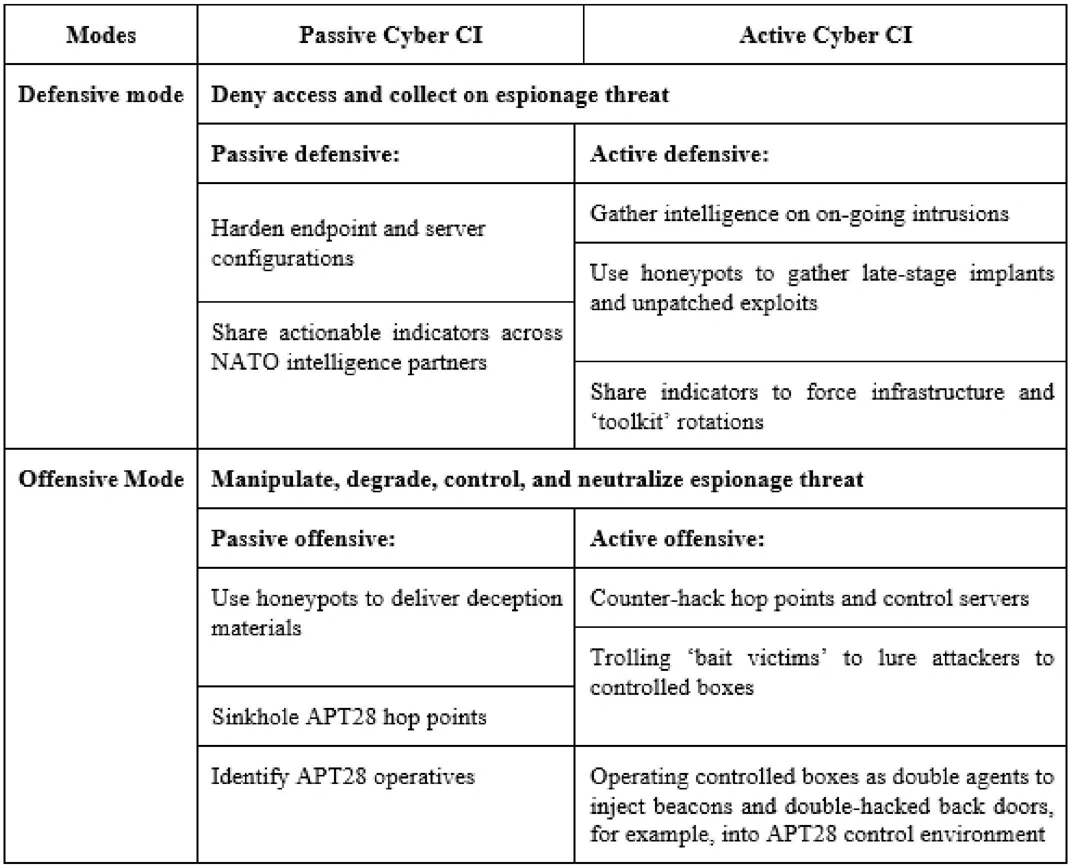
This section discussed the CCI levels of execution within within the CCI matrix's vertical plane. The next section illustrates the matrix's application by means of the Stech and Heckman (2018) hypothetical case study.

The CCI Matrix in Practice—A Hypothetical Case Study

As was observed earlier in the article, the organisation's CCI posture on the strategic level (interests, goals, and strategy) will shape CCI activities on the operational and tactical-technical levels. It then logically follows that strategy and operational objectives will determine the offensive-defensive, passive-active modes on a tactical-technical level. This point, as well as the application of the authors' CCI matrix, are illustrated by the Stech and Heckman (2018) proposition on a 'cyber counterintelligence framework in active defense'. Utilising a hypothetical case study of a NATO campaign against Advanced Persistent Threat (APT) actors associated with Russia, APT28 and APT29, Stech and Heckman (2018) pose the following as NATO's strategic CCI goal and operational objectives:

- Support NATO strategic deception goal: Convince Russian authorities their cyber intelligence supports propaganda but is not ready for kinetic war against NATO.
- Active & Passive CCI Defense: Reduce and eliminate effectiveness of APT28 tactics, techniques, and procedures for espionage. Eliminate or counter APT28 and APT29 malware and tradecraft.
- Passive CCI Offense: Poison APT28 and APT29 intelligence stream with deception materials; eliminate, corrupt, or covertly take over control of attackers' command and control.
- Active CCI Offense: Feed Russian espionage units with false information (such as feed APT29 false information about actions and effects of APT28, and vice versa).
- Support apparent intrusion successes with cyber and non-cyber strategic NATO deception operations.

In extending the strategic goal and operational objectives to the tactical-technical level, Stech and Heckman (2018) apply the four-sector matrix (advanced per **Figure 3**, above, and further developed in **Figures 4** and **5**, above, of this article) to the hypothetical NATO-Russia case study. This is done by means of the table in **Figure 7**, below.



Modes	**Passive Cyber CI**	**Active Cyber CI**
Defensive mode	**Deny access and collect on espionage threat**	
	Passive defensive:	**Active defensive:**
	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 neutralize 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 and double-hacked back doors, for example, into APT28 control environment

Figure 7: Hypothetical NATO cyber CI operations against cyber espionage threat (Stech & Heckman 2018)

This section illustrated the application of a four-mode, three-tiered CCI matrix by citing Stech and Heckman's (2018) hypothetical NATO case study. The article now proceeds with observations on the CCI matrix's context and significance.

Conclusion

This article is written within the context of non-state entities' growing adoption of CCI in the face of escalating targeting by intelligence actors of various categories. CCI undoubtedly offers a prac-ticable approach to protect and advance organisational interests. There is, however, a precondition and qualification. Unless it is meticulously configured, CCI is more likely to be self-defeating than beneficial. This article advanced a CCI matrix which hopefully could aid the configuration of a robust cybersecurity posture and the exploitation of opportunities. On an academic level, the CCI matrix might be useful to conceptually structure aspects of research in this fast-growing field.

References

Coats, D 2018, *Worldwide threat assessment of the US intelligence community*, viewed 27 July 2018, <https://www.dni.gov/files/documents/Newsroom/Testimonies/ 2018-ATA---Unclassified-SSCI.pdf>.

Duvenage, P 2019, A conceptual framework for cyber counterintelligence, unpublished Doctor of Commerce (DCom) thesis, University of Johannesburg, Johannesburg, ZA.

Duvenage, P & von Solms, S 2013, 'The case for cyber counterintelligence', Proceedings of the 5th International Conference on Adaptive Science and Technology, Pretoria, ZA.

——2014, 'Cyber counterintelligence: Back to the future', Journal of Information Warfare, vol. 9, no. 3, pp. 42-56.

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

Jaquire, V 2018, A framework for a cyber counterintelligence maturity model, unpublished Doctor of Commerce (DCom) thesis, University of Johannesburg, Johannesburg, ZA.

Jaquire, J, Duvenage, P & von Solms, S 2018, 'Building the CCI dream team', Proceedings of the 17th European Conference on Cyber Warfare and Security, Oslo, NO.

Panda Security 2018, The hunter becomes the hunted: How cyber counterintelligence works, viewed 6 November 2018, <https://www.pandasecurity.com/mediacenter/panda-security/cy-ber-counterintelligence>.

Prunckun, H 2012, *Counterintelligence: Theory and practice*, Rowman & Littlefield Publishers, Plymouth, UK.

Sims, J 2009, 'Twenty-first-century counterintelligence', *Vaults, mirrors and masks—Rediscover-ing U.S. counterintelligence*, J Sims & B Gerber (eds), Georgetown University Press, Washington D.C., US.

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.

Symantec 2018, *Internet Security Threat Report Volume 23 - March 2018*, viewed 03 March 2019, <https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-executive-summary-en. pdf>.

Symantec 2019, *Internet security threat report, volume 24, February 2019*, viewed 17 June 2019, <https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-executive-summary-en.pdf>.

van Niekerk, B & Duvenage, P 2016, 'Cyber intelligence and counterintelligence', *ISACA South Africa Conference 2016*, Johannesburg, ZA.