Indexed in: Web of Science Emerging Sources Citation Index (ESCI), SCOPUS, Google Scholar, ProQuest and 12 more indices
ISSN: 1947-3435|EISSN: 1947-3443|DOI: 10.4018/IJCW

International Journal of Cyber Warfare and Terrorism (IJCWT)

Volume 9 • Issue 4 • October-December 2019

Cyber Counterintelligence - An Exploratory Proposition on a Conceptual Framework

Petrus Duvenage, University of Johannesburg, Johannesburg, South Africa

Thenjiwe Sithole, University of Johannesburg, Johannesburg, South Africa

Basie von Solms, University of Johannesburg, Johannesburg, South Africa

International Journal of Cyber Warfare and Terrorism
Volume 9 • Issue 4 • October-December 2019

Cyber Counterintelligence
An Exploratory Proposition on a Conceptual Framework

Petrus Duvenage, University of Johannesburg, Johannesburg, South Africa

Thenjiwe Sithole, University of Johannesburg, Johannesburg, South Africa

Basie von Solms, University of Johannesburg, Johannesburg, South Africa

ABSTRACT

This article advances a conceptual framework for cyber counterintelligence (FCCI) as a theoretical construct, hopefully useful not only to this field's academic development, but also to sound practice. It is submitted within the context of the sharp increasing targeting of state and non-state actors by adversarial intelligence actors (such other nation states, crime syndicates and competitors). The signature role of cyber counterintelligence (CCI) is precisely the engagement, exploitation and neutralisation of such adversarial actors. CCI has been practised by nation states for well over a decade and has recently also been gaining traction in corporate board rooms and as an academic field. Sound theory is critical to not only CCI's academic evolvement but also to sound practice. The proposed FCCI comprises of eight notional building blocks essential to explaining what CCI is and how it works.

KEYWORDS

Active Defense, Cyber Counterintelligence, Offensive Cybersecurity, Strategy, Theory, Threat Intelligence

DOI: 10.4018/IJCWT.2019100103

1. INTRODUCTION

The targeting of nation states and non-state organisations with high-value information assets by intelligence actors (such nation states, crime syndicates and competitors) continues its sharp increase. In 2019, for example, Symantec reported that the number of "Targeted Attack Groups", the vendor is tracking, rose to 155 – an astounding 78% increase from the 87 groups monitored in 2015 (Symantec, 2018; Symantec, 2019). Symantec (2019) states "intelligence gathering" as the primary motive behind 96% of attacks by these groups. Also, Kaspersky (2018) confirmed the rising concern over targeted attack groups. According to a recent survey, 66% of companies view "targeted attacks/ [Advanced Persistent Threats] APTs" as their foremost cybersecurity concern.

The signature role of cyber counterintelligence (CCI) is precisely the engagement, exploitation and neutralisation of such targeted attack groups and APTs. Properly conceptualised and implemented as part of counterintelligence, CCI is a practicable approach for governments, businesses and other sizable entities. The demand for, and on, CCI is sure to increase (Economist, 2015; Panda Security Labs, 2018).

While practitioners and executives engaging high-end adversaries in the 'real world' are progressively warming up to the opportunities CCI presents, the mentioning of 'theory' is likely to evoke a cool response. Theory is typically regarded as abstract thinking that has little bearing on, or use in, 'real world' cybersecurity trenches. Theory may even be deemed to be the opposite of practice. This is of course not the case – theory is highly relevant to practice and practice ought to inform theory. In the words of Lewin (as cited by Greenwald, 2012): "There is nothing so practical as a good theory."

Especially for a field as complex as CCI, effective practice presupposes a sound theoretical foundation. The price for poor CCI theory will ultimately be paid through more costly failures and damaging breaches. Theoretical constructs are thus clearly not 'nice to have' academic 'toys'. These constructs, which include frameworks and models, condition our thinking and our approach to practice. In addition to its application to practice, theory should of course also be at the heart of academic disciplines and fields.

Herein lies the challenge – as an emerging multi-disciplinary academic field, CCI is in its infancy. Given CCI's incipient status, one of the priority agenda items ought to be a conceptual framework that (albeit tentatively) delineates and provides a coherent view of the research object – i.e. CCI. This conceptual framework can furthermore systemise existing knowledge and provide a scaffold for further research. Equally important, it can be an instrument to explain to diverse audiences what CCI is and how it works. This paper's primary aim is to advance the outlines of such a conceptual Framework for CCI (FCCI). The FCCI consists of eight notional blocks essential to an academic credible and practically useful FCCI.

The article sets off with explaining and contextualising the approach followed in the FCCI's design. This is addressed in Section 2 and 3. Section 2 defines a 'conceptual framework' and describes how this fits in with 'theory'. The article then proceeds with discussing the requirements to which the design of an academic credible and practically useful FCCI should comply (Section 3). Guided by these requirements, Section 4 outlines the FCCI and its eight building blocks. The article concludes with observations on future CCI research (Section 5).

2. WHAT IS A ’CONCEPTUAL FRAMEWORK’ AND HOW DOES IT FIT IN WITH ‘THEORY’?

The FCCI’s design has a prerequisite clarity on what a ‘conceptual framework’ is and how this fits in with ‘theory’. To this end, this section firstly reflects on the notion ‘theory’ and then proceeds to define a ‘conceptual framework’.

In a general sense, ‘theory’ can be described as the interrelated collective of definitions, concepts, constructs (i.e. models and frameworks) as well as propositions to explain and understand a phenomenon/phenomena and/or aspects thereof. It is important to note that the ‘theory’ of an academic subject is not always a homogeneous body of thinking, but more often competing bodies of thinking. These bodies of thinking vary in their focuses from the abstract and broad to the more concrete and specific. Postulations on the meta-paradigm and paradigmatic levels are abstract and broad in scope, while meso-theories are more concrete and specific. These layers of theories’ different purposes are aptly summarised by Gill (2006) in his distinction between “theories of intelligence” and “theories for intelligence.” “Theories of intelligence” asserts Gill (2006), are developed to “help academics research intelligence, come to understand it, and better explain it”. Theories for intelligence “relate immediately to the needs of practitioners” ... In one sense there is no conflict between these two. A good theory of intelligence should, by definition, be useful for intelligence.”

Within the above context, a ‘conceptual framework’ can broadly be defined as a theoretical construct that narratively and/or graphically conveys the “essential or underlying structure, a provisional design, an outline; a connectional scheme or system” of a particular study object (Oxford Dictionary, 2016). While a conceptual framework is per definition skeletal and tentative, it can nonetheless “provide a comprehensive understanding of a phenomenon. Conceptual frameworks are [thus] not merely collections of concepts but, rather, constructs in which each concept plays and integral role” (Jabareen, 2009). A conceptual framework can serve as (i) a theory of a study object, (ii) theory for a discipline and (iii) a combination of these two.

Moving from this general definition, the FCCI advanced in this article can simply be defined as a theoretical schema that explains CCI by means of a collection of concepts (i.e. building blocks). As will be shown in Section 4, the FCCI is for the most part a theory for CCI, but also includes elements of abstract, higher-order theories.

3. A ’CONCEPTUAL FRAMEWORK FOR CCI’ – WHAT IT SHOULD DO AND WHY IT MATTERS

The foregoing description of a conceptual framework provides a foundation for deriving the requirements to which the FCCI should comply. Essentially, the requirements are a response to the question: What should the FCCI look like and what should it be able to do (functions)? The requirements will guide the FCCI's design in Section 4. Ultimately the application of these requirements determines the FCCI's effectiveness, uses and benefits. It is these benefits that demonstrate why the FCCI is a theoretical construct that ought to matter for academics and practitioners.

The FCCI's requirements, functions and benefits are closely related and overlapping. In the interest of simplicity we addressed all these by means of the following consolidated list in which we assert that the FCCI should:

- Be academically credible and practically useful.
- Graphically and narratively, describe what CCI is, of what it comprises (building blocks) and how it works.
- Be simultaneously "congruent with reality and an idealised, simplified representation of reality." (Duvenage, von Solms, Corregedor, 2015). Since it is an idealisation, the FFCI has to be an aiming point of what CCI should encapsulate if executed flawlessly.
- Serve as a conceptual template for CCI practice and its synergetic execution with the broader organisational endeavour.
- Be a nexus for linking CCI with other fields of practice and multi-disciplinary academic enquiry.
- Position itself as part of the theoretical discourse.
- Be scalable in that it should be able to explain CCI on the strategic, operational, tactical and technical layers.
- Serve as a scaffold to structure knowledge and research.
- Be derived through a qualitative (grounded theory) process that draws on the researcher's experiential knowledge, existing theory and research.
- Be qualified as a tentative artefact that is subject to validation and constant modification.

This section listed criteria which should be considered in the FCCI's design.

4. AN OUTLINE OF THE CONCEPTUAL FRAMEWORK FOR CYBER COUNTERINTELLIGENCE (FCCI)

Guided by the criteria discussed above, this section designs and advances an outline of the FCCI. The FCCI is presented by means of a progressive block-by-block construction of the framework. At each of the respective building blocks, we:

- Graphically, depict the addition of the building block to the FCCI.
- Explain why the particular building block is essential to the FCCI.
- Offer a cursory outline (contours) of the building block in question. This outline comprises of a brief description/definition of concepts and a brief mentioning of facets that can direct further research and theorisation.

The paragraph above described our approach to presenting the FCCI in this paper. We now proceed with discussing the first building block namely a 'Theoretical Anchor'.

4.1 Building Block 1: Theoretical Anchor

Graphically the FCCI's theoretical anchor can be depicted in Figure 1:

4.1.1 Why is this Building Block Needed?

To be academically credible the FCCI has to duly consider and position itself as part of the existing theoretical discourse. Such anchoring provides a nexus for linking CCI with other academic fields. The anchoring of our FCCI in theory is also important from a practical point of view. As was noted earlier, theory conditions our thinking and thus our approach to practice. Consequently, the theoretical anchor will determine both the way in which we design the rest of our FFCI and ultimately CCI practice.

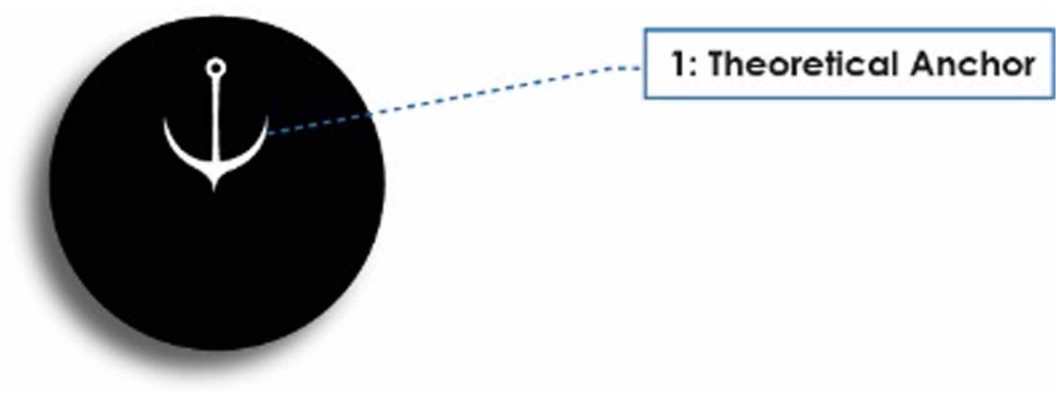
4.1.2 Building Block Contours

Section 2 and 3 explained the FCCI predominantly as a theory on a lower level of abstraction. Accordingly, the FCCI's first building block comprises the linking of the FCCI with levels of higher abstraction, namely on the meta-paradigmatic, paradigmatic, theory and meso-theory levels. The building block has to clearly indicate the core theoretical contentions on which the FCCI is based.

Although CCI is a multi-disciplinary field, it has its primary taproot within Intelligence Study and Political Science (notably International Relations) theory. Intelligence and Political Science theory is of course not a homogenous body of thinking and the discourse is one of competing narratives that include Realism, Liberalism, Constructivism, Radicalism and Poststructuralists. In our view, Realism best explains Intelligence, CI and CCI (*cf*. Duvenage & Hough, 2011). Through a Realist lens, the contours of the FCCI's first building blocks are as follow:

- On the meta-paradigmatic level, the FCCI subscribes to a positivist position. Accordingly, an objective world (reality) is deemed to exist separately from the

Figure 1. Building block 1 – theoretical anchor



researcher/practitioner. Extended to the FCCI, we assert that this framework can objectively identify, describe and guide the pro-active mitigation of 'real' threats and risks to the Organisation.

- On the paradigmatic layer, we take a realist stance as was mentioned prior. Therefore, the state (or more generically the 'organisation') is seen as a rational, self-interested entity driven by the pursuit of its security and expanding its vital interests vis-à-vis other actors. The organisation's relative power is a key factor in this quest. These vital interests are pursued against other actors in the political, social, technological, economic, military, ecological (environmental) and information sectors. Intelligence and cyber form part of the information sector.
- Extending realism to the grand theory level, we view intelligence as simultaneously a class of vital interests and category of power. Within this context 'cyber' is exponentially increasing its centrality as a tool and asset.
- On the meso-level, counterintelligence and therefore CCI, is the Intelligence element tasked with protecting and advancing the organisation's interests in the face of other role-players' hostile intelligence actions.

Properly designed the first building block, presented above, serves as a theoretical roadmap for the design of further FCCI building blocks. Since building blocks repeat and expand different theoretical positions, building block 1 acts as the central notional node that binds all further FCCI theory. It is thus the anchor to which all further blocks relate.

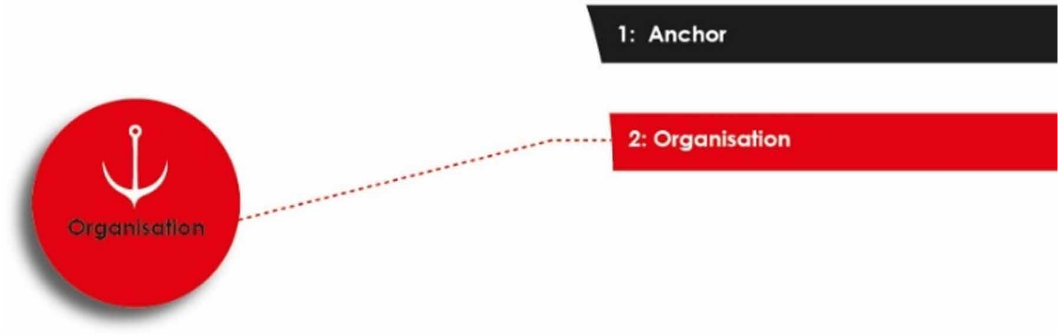
4.2 Building Block 2: Organisation

With the CCI theoretically anchored, the FCCI's pivot - that is the organisation - can be constructed. Graphically, this building block can be depicted in Figure 2:

4.2.1 Why is the Building Block Needed?

The organisation is advanced as the FCCI's pivot for reasons of theory and practicality. In line with Realist theoretical position, the organisation and the pursuance of its interests predominate. Seen through this lens, CCI is ultimately about maximizing

Figure 2. Building block 2 – the organisation



the organisation's power through protecting and advancing interests. Therefore, CCI exists because of, and for the organisation, it serves. Also, practically, effective CCI crucially depends on a profound knowledge of the organisation. Against sophisticated adversaries, for example, the organisation's staging of honeynets and the content filling of honeypots, honeyfiles and honeytokens have to be attuned to the organisation's itself, its adversaries and its environment (Bodmer et al., 2012; Duvenage & von Solms, 2013).

4.2.2 Some Building Block Contours

The 'organisation' is a generic concept that can refer to various types of entities, ranging from nation states and multi-national corporates to smaller businesses and non-governmental organisations. Regardless of the type of entity we are dealing with, aspects to be addressed in explicating the organisation as an FCCI building block are the following:

- The organisation's vision, goals and the vital interests it wants to protect and procure in order to be more secure and prosperous. Although these vital interests exist in various domains, it is central to the later configuration of the CCI effort, to identify and concretely describe vital informational interests.
- The organisation's strategy for pursuing its vision and objectives.
- Organisational strengths (inclusive of the vital interests and instruments of power it possesses) and weaknesses (vulnerabilities). Also, in this case, particular attention should be given to the information sphere.
- The environment in which the organisation functions. Of particular importance are the implications of current as well as anticipated trends on the organisation reaching its objectives and expanding prosperity.
- Actual and potential competitors/adversaries and, also in this instance, the implications thereof on the organisation attaining its objectives.

This subsection discussed the addition of the 'organisation' as an FCCI building block. Within the context of the latter, CCI is but part of a much broader organisational endeavour, namely Intelligence. The next subsection therefore proposes Intelligence as the FCCI's subsequent building block.

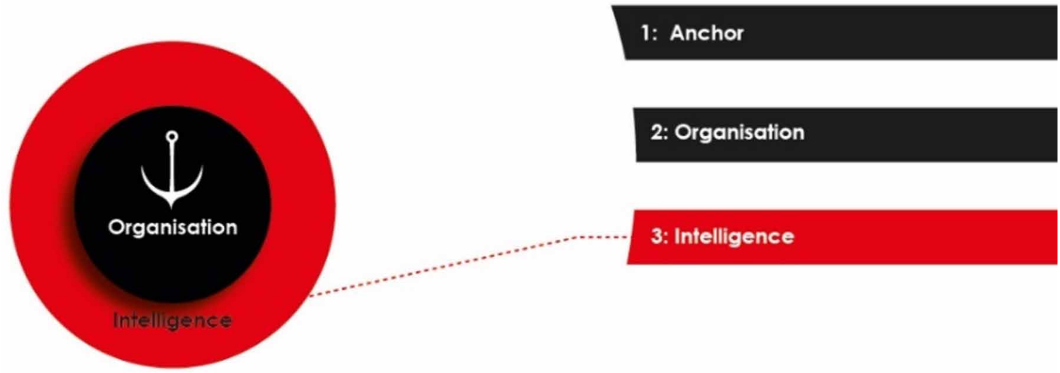
4.3 Building Block 3: Intelligence ('Toolkit')

Graphically, the addition of intelligence as an FCCI building block can be depicted in Figure 3:

4.3.1 Why the Building Block is Needed?

While an indispensable instrument, CCI cannot secure and pursue an organisation's interests all by, and for, itself. This has to be done as part of an organisation's Intelligence endeavour. CCI, by way of analogy, is but one 'tool type' within an organisation's Intelligence 'toolkit'. Academia and practitioners serious about CCI have

Figure 3. Building block 3 – intelligence



to have a sound grasp of Intelligence (toolkit) as well as Intelligence's three toolsets (Positive Intelligence, Covert Action and Counterintelligence). Since these are also performed within CCI, clarity is furthermore needed on Intelligence functions (such as management, analysis and collection).

4.3.2 Building Block Contours

In order to contour 'intelligence' as an FCCI building block, it needs to be defined. With the qualification that there is no commonly accepted description, the following definition of 'intelligence' offer by Lowenthal (2012) will suffice for purposes of this article:

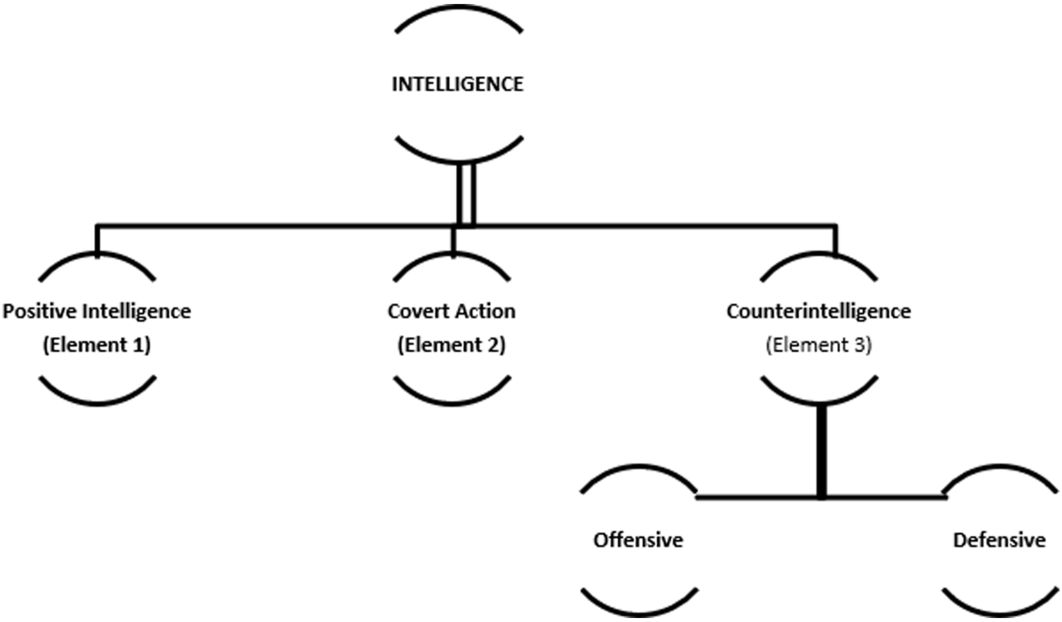
Intelligence is the process by which specific types of information important to an organisation's vital interests are requested, collected, analysed, and provided to the decision makers, the products of that process; the safeguarding and advancement of informational interests by counterintelligence activities; and the carrying out of other sanctioned informational operations.

Underpinning the above definition is the notion that intelligence (toolkit) consists of the three interrelated elements (toolsets). These three elements constituting the Intelligence trident depicted in Figure 4:

The three Intelligence elements can be concisely be described as follow (Duvenage, 2019 – verbatim extract):

- **Positive intelligence** is primarily aimed at providing information "to facilitate one's own side achieving its ends" (Bodmer et al., 2012). This information varies from analysed open sources to an opponent's secrets obtained through espionage. As noted above, 'intelligence' is frequently used interchangeably as referring to 'positive intelligence', with the context determining what meaning is implied (Sims, 2009). From our explanation in the two bullet points directly following this one, it is abundantly clear that Intelligence is about much more than delivering actionable knowledge about opponents and the environment. It also entails covert action and CI – whether executed by state or non-state actors.

Figure 4. The intelligence trident (Duvenage, von Solms & Corregedor, 2015)



- **Covert action** targets an adversary by influencing events, conditions, individuals, groups or institutions to the benefit of the client and in a manner not attributable to the sponsor or at least offering plausible deniability (Duvenage, von Solms & Corregedor, 2015). To this end, measures instituted "are to one degree or another secret (hidden) or covert (disguised)" (Godson, 2001). In the context of state security, covert action can include action such as military and intelligence interventions and support. In state intelligence structures, covert action mostly relates to informational actions such as propaganda, deception and disinformation (Godson, 2001). In the business environment, some forms of deception and 'perception management' could in effect be forms of covert action
- **Counterintelligence** (CI) is an abbreviated form of countering hostile intelligence activities. CI defensively and offensively guards against adversarial intelligence (i.e. hostile positive, CI and covert action) operations (Duvenage, von Solms & Corregedor, 2015; Prunckun 2012; Sims, 2009). CI thus pertains to the safeguarding of the own organisation's weaknesses and vulnerabilities as well as the active engagement of adversaries.

Traversing and performed in all toolsets, are specialised intelligence functions such as management, analysis and collection. These Intelligence functions, which are also performed within CCI, bind the three Intelligence elements.

Since the foregoing explanation is but a cursory contour, it risks being an oversimplification. A thorough explication of Intelligence as an FCCI building block will have to describe concretely the synergy between, on the one hand CCI, and, on the other hand, Intelligence elements and functions. It will explain how CCI depends on and benefits from all three Intelligence elements. Of these elements, and for reasons discussed below (Section 4.4), CI and its relationship with CCI are of particular importance. So important in fact, that CI is advanced in the next section as a distinctive CCI building block.

4.4 Building Block 4: Counterintelligence ('Toolset')

Graphically, the addition of Counterintelligence (CI) as the FCCI's fourth building block can be depicted in Figure 5:

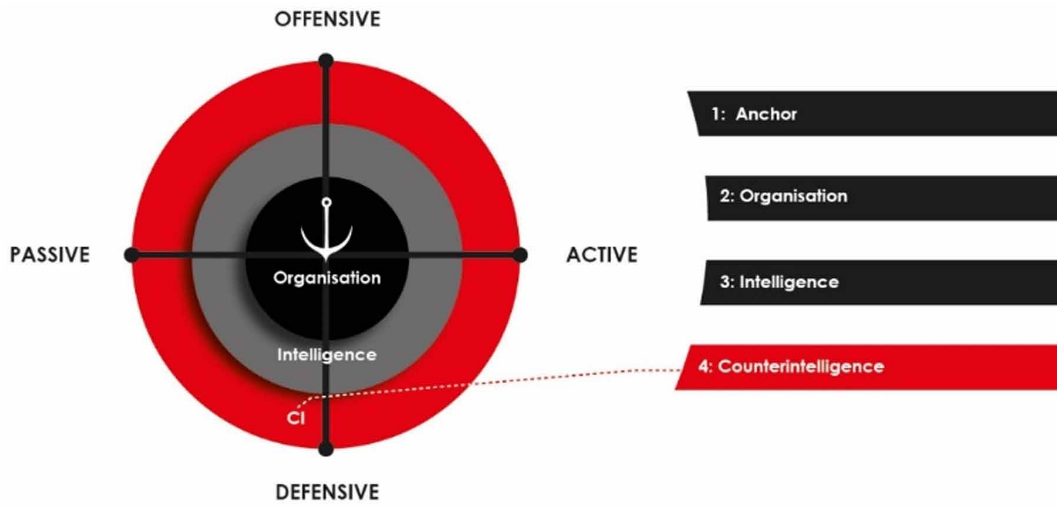
4.4.1 Why the Building Block is Needed?

In the preceding section we positioned CI (and thus CCI) as part of an Organisation's Intelligence endeavour. In this section we advance CI as the subsequent building block of our FCCI because we cannot conceptually structure and understand CCI, if we do not understand CI of which CCI is part. CCI is by way of analogy one of the 'tool types' within the CI 'toolset'. Practically and conceptually, CCI is linked with the whole of the multidisciplinary CI effort. CCI is, in other words, not a neat compartment within CI. It involves, and requires clarity of, all other CI fields.

4.4.2 Some Building Block Contours

To delineate CI as an FCCI building block, we also in this instance offer a definition. Expanding on earlier contributions (Duvenage & von Solms, 2013; Duvenage, Jaquire & von Solms, 2016), we define CI for purposes of this paper as the collective of measures an Organisation undertakes to identify, deter, exploit, degrade, neutralise and protect against adversarial intelligence activities and internal risks deemed as detrimental or potentially detrimental to the organisation's vital informational interests and the pursuance thereof. Such hostile intelligence actions "include espionage as

Figure 5. Building block 4 – counterintelligence



well as other actions that could degrade the integrity and/or availability of valued information, information systems and processes" (Duvenage & von Solms, 2014). Differently phrased, the adversarial intelligence that CI engages comprises of adversarial positive intelligence (inter alia espionage), covert action and adversarial CI. To perform this role, CI relies on a wide range of measures. CCI is involved in, and is in some way or another, reliant on most CI measures (see third bullet in paragraph below – Five clusters of CI measures).

In order to explain CCI, this building block has to describe CCI's link and relation with the whole of the CI endeavour. To this end, aspects that have to be addressed and their application to cyber explained, include but are not limited to the following:

- CI principles and doctrine.
- CI's offensive and defensive missions as well as CI's passive and active modes (Prunckun 2012, Duvenage & von Solms 2015, Duvenage, Jaquire & von Solms, 2016).
- The clusters of CI measures namely (i) Physical Security, (ii) Information and Technological Systems Security, (iii) Personnel Security, (iv) Counterintelligence Monitoring, Investigation, and Collection; and (v) Counterintelligence Exploitation, Deception and Neutralisation (Prunkun, 2012; Duvenage, 2013)
- The difference and interplay between strategic, operational and tactical CI.

In this section CI was advanced as an FCCI building block. In the next section we submit the FCCI fifth component, namely CCI.

4.5 Building Block 5: Cyber Counterintelligence ('Tool set')

The addition of CCI as the FCCI fifth building block can be graphically illustrated in Figure 6:

4.5.1 Why the Building Block is Needed?

In order to illustrate the interlock between CI and CCI, the diagram above deliberately depicts the two fields in the same ring and on the same level. This is done to graphically reflect this paper's recurring theme namely that CCI is but a tool type within the broader CI toolset. Hence, CCI is defined as "that subset of multi-disciplinary CI aimed at detecting, deterring, preventing, degrading, exploiting and the neutralisation of adversarial attempts to collect, alter or in any other way breach the C-I-A [confidentiality, integrity and availability] of valued information assets through cyber means and/or where cyber assets are targeted" (Duvenage, von Solms, & Corregedor, 2015). As is clear from this definition and the term cyber counterintelligence, this FCCI building block explicates CCI as a technical toolset. This toolset comprises of an extensive range of tools (technologies, measures and techniques). Most of these tools are not unique to CCI. What is unique is the application thereof in combination with other CI tools and in a manner best achieving CI's missions.

4.5.2 Some Building Block Contours

A more detailed explication of CCI as an FCCI building would therefore entail the describing of the application to the CI context of the said technologies, measures and techniques. The following (Table 1) serve as some examples (Bodmer et al., 2012: Heckman et al., 2015; Jaquire, 2018).

Being the FCCI's technical toolset, this building block (and the subsequent blocks discussed in Section 4.6, 4.7 and 4.8) need to be configured with due consideration of, but also distinctly move beyond, existing cyber-security standards, guidelines and frameworks. These include for example, (as a non-exhaustive list), those prescribed in/by NIST, COBIT, ITIL, ISA/IEC, CIS, OWASP, FFIEC and ISO (e.g. 27001, 27002). Serving as further examples are the guidelines advanced per the STIGs (US Department of Defence Security Technical Implementation Guides), as well as technical security configuration guides by as provided by the NSA and/or similar bodies (Jaquire, 2018).

This subsection advanced and contoured CCI as an FCCI building block. The next subsection adds the CCI matrix as a further building block.

4.6 Building Block 6: CCI Matrix

Graphically the adding of the CCI matrix to the FCCI can be illustrated in Figure 7:

Figure 6. Building block 5 – cyber counterintelligence

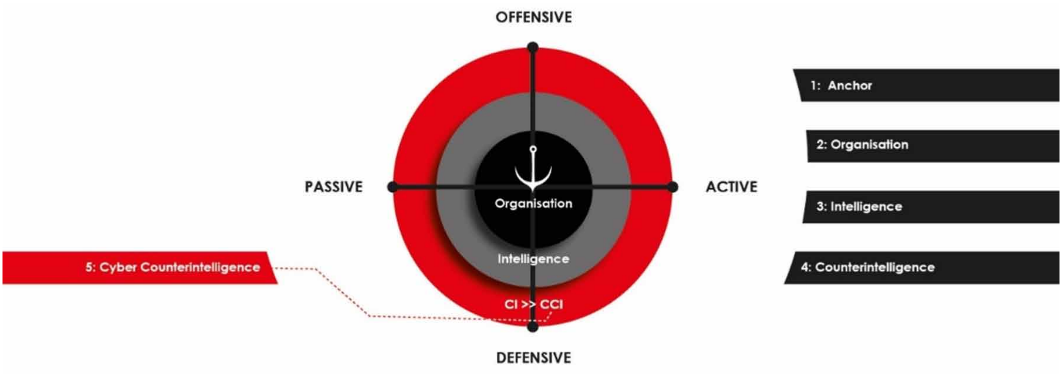
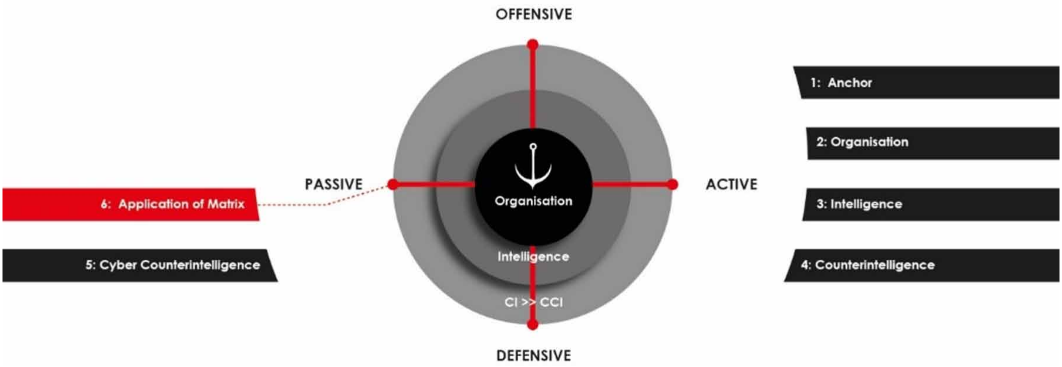


Table 1.

■ Host–based tools (Antivirus, Digital forensics, Security management tools) ■ Network-based Tools (Firewall, IDS/IPS) ■ Incident Management and coordination (Detection, Analyses, Response, Recovery). ■ Profiling, Attribution and Decisions models. ■ Data mining, modelling and reporting tools ■ Sock puppets as tools of collection, deception, influencing and neutralisation. ■ Scripting, penetration, hacking and exploitation.	■ Active engagement procedures (Internal and External to network). ■ Denial and Deception Technologies (tarpits, black holes, honeynets, honeywalls, content staging and filling). ■ Malware analysis, engineering, reverse engineering and development. ■ Insider Cyber Threat Mitigation tools and measures. ■ Cyber Supply-Chain Management (Aligned to threats and opportunities).

Figure 7. Building block 6 – application of the CCI matrix



4.6.1 Why the Building Block is Needed?

Subsection 4.5 noted that CCI tools should be used in a manner best achieving CI offensive and defensive missions. CCI tools can seldom be pigeonholed as having only a defensive or an offensive purpose. In various instances they can be useful to more than one. Furthermore, a significant part of tools can be deployed in an active or passive mode. To add to the complexity, effective CCI requires the integrated execution of offensive/active and defensive/passive modes. They can, after all, be described as different sides of a cube. The configuration of the CCI's passive-active and defensive-offensive endeavour is complex and unique to each Organisation. Lastly, effective CCI is executed on three levels, namely the strategic, operational and tactical –technical. In order to explain and guide this complex configuration and deployment of CCI tools, we require a conceptual construct as part of the FCCI.

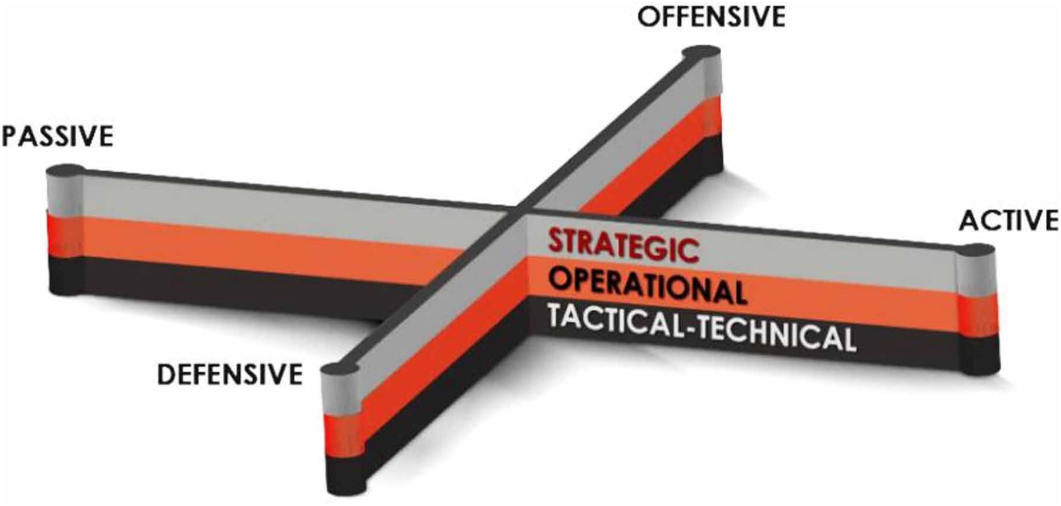
4.6.2 Some Building Block Contours

To meet this requirement, the FCCI advances, a three-dimensional, four-quadrant matrix as such a conceptual construct. Diagrammatically, the CCI matrix can be depicted in Figure 8:

The CCI matrix's horizontal plane depicts the four quadrants which represent the CCI posture's four modes, namely: Passive-defensive, Passive-offensive, Active-defensive and Active-offensive. Similar to several other constructs, this matrix is derived from multi-disciplinary CI. A more detailed description of the matrix as an FCCI building block would firstly involve the narrative description of each of the four quadrants. Secondly, the matrix will have to be populated with the CCI tools available, and in accordance with the CI needs of the Organisation. Concretely the matrix's population entails the plotting on the matrix of CCI tools. Ideally, the plotting of the matrix would be informed by a taxonomy of CCI tools.

The matrix's vertical plane (i.e. Figure 8's three layers) integrates CCI with the broader organisational, intelligence and CI endeavour at the various levels on which CCI functions. This is done by describing CCI's execution on three organisational levels/layers, namely: (1) Strategic, (2) Operational and (3) Tactical/Technical. Within

Figure 8. CCI matrix (Duvenage, Jaquire & von Solms 2019)



the confines of this article these levels and their unique challenges cannot be described. For a more detailed explication of the CCI matrix and its practical application see Duvenage, Jaquire & von Solms (2019).

In this subsection, the CCI matrix was explicated as the FCCI's sixth building block and we now proceed with introducing 'Delineation and Cooperation' as the next component.

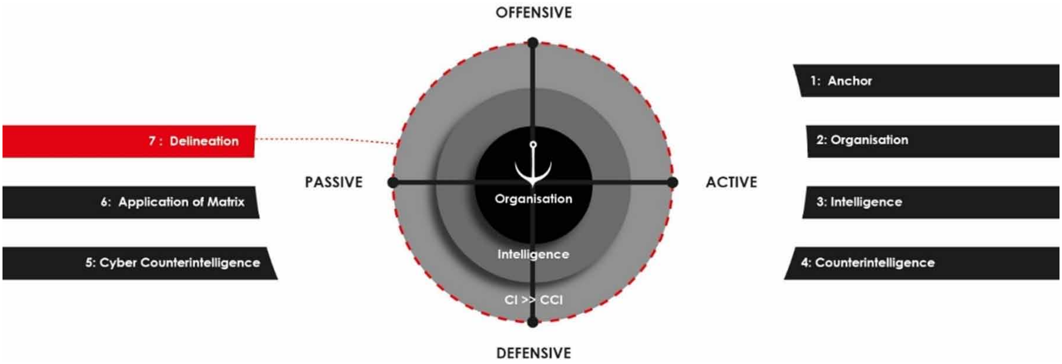
4.7 Building Block 7: Delineation and Cooperation

We can illustrate the addition of 'Delineation and Cooperation' as the FFCI's next building block in Figure 9:

4.7.1 Why this Building Block is Needed?

By its very nature, the cyber-sphere is one of an interconnected reality. Even with all the previous building blocks in place, an Organisation would seldom be able, or

Figure 9. Building block 7 – delineation and cooperation



legally allowed, to execute the whole of the CCI endeavour on its own. Business entities would, for example, be legally prohibited and not have the resources to undertake some active-offensive cyber campaigns undertaken by nation-states. In a similar vein, nation-states have to cooperate with non-state actors to achieve national goals. Consequently and although ultimately driven by each actor's self-centred interests, effective CCI requires cooperation with other actors and a delineating respective roles.

Delineation is also important in the academic context. Treating CCI as a too wide and encompassing field will result in the loss of focus. Simultaneously, CCI must be clear on its relation with various other academic subjects and on the areas of multi-disciplinary research.

4.7.2 Some Building Block Contours

The 'Delineation and Cooperation' building block typically consists of a narrative description of areas of cooperation. In the academic arena, comparative studies and multi-disciplinary research are useful for refining CCI's focus and exploring areas of cooperation.

In this part, we proposed 'Delineation and Cooperation' as the FCCI's seventh building block. In the subsection to follow, we discuss the CCI building block, namely the CCI process.

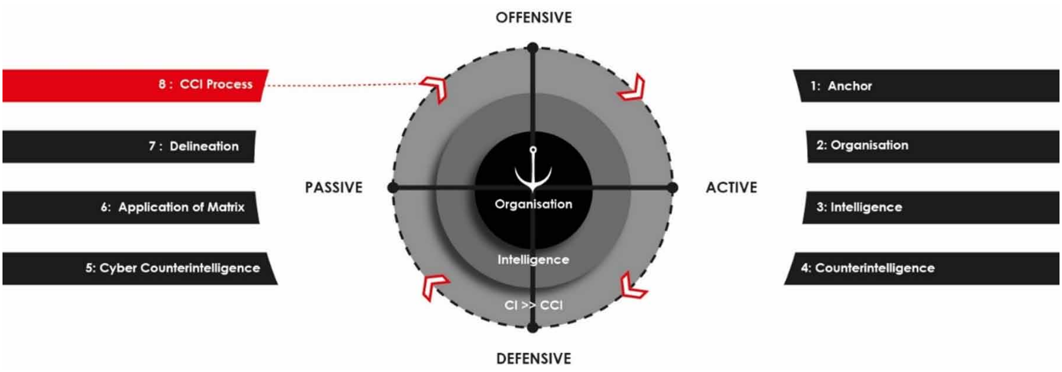
4.8 Building Block 8: CCI Process

The addition of the CCI Process as the FCCI's eighth and last building block can be depicted in Figure 10:

4.8.1 Why this Building Block is Needed?

Properly contextualised, the foregoing building blocks provide all the 'parts' necessary to academically explain and practically execute CCI. At this juncture, these parts – and thus the FCCI – are still 'static'. They lack the dynamism that synergistically combines and drives these different parts as an integrated process. Consequently, the FCCI proposes a CCI process model as its last component.

Figure 10. Building block 8 (process) completing the conceptual framework for cyber counterintelligence (FCCI)



4.8.2 Some Building Block Contours

A process model typically consists of a graphically depicted and narratively explained step-by-step action. Seeing that its part of Intelligence and CI, the design of the CCI process has to consider existing propositions on the Intelligence, CI and CCI processes. In a previous contribution, some salient existing propositions were evaluated and found not to sufficiently explain CCI. These propositions, neither "reflect the defensive and offensive counterintelligence thrusts" nor are they "granulated enough to serve … as an aiming point for practical execution or a sounding board for further academic exploration" of a CCI process model (Duvenage, von Solms, & Corregedor, 2015). The said authors proceeded with presenting the contours of a process model that consists of a flow diagram and a narrative description of the CCI process. This model, albeit on a high level, provides the contours of a workable CCI process model.

In this section we presented our FCCI by means of progressive block-by-block construction. In the next section, we conclude with observations on further research.

5. CONCLUSION

This article's aim was to present the approach to, and outlines of, a conceptual Framework for Cyber Counterintelligence (FCCI). In the 'real world' of cybersecurity practice, CCI is an intricate field. CCI is distinctive from, yet intertwined with, various other specialisation fields. Its successful execution, therefore, depends on diverse skillsets. Within this diversity and intricacy, we risk losing clarity and focus. The FCCI we advanced is hopefully a simplified notional construct with some explanatory power. Although not possible to illustrate within the confines of this article, outcomes of our FCCI's application to several major and recent cyber breaches do affirm this framework's academic credibility and practical application to 'real world' incidents.

Being a conceptual framework, the FCCI is nonetheless subject to refinement. This refinement requires constructive criticism and further research. While the FCCI is explicated in much more detail in research at the University of Johannesburg (Jaquire, 2018; Duvenage, 2019) and positive feedback was received, there is vast, fertile ground for further academic exploration. Themes for such research could include the application of the FCCI for training purposes. In respect of CCI more generally, a foremost priority item on the research agenda ought to be the interface and dynamics between CCI and information/cyber warfare. Currently, and with very few notable exceptions (e.g. Justiniano, 2017), even outstanding works on information and cyber warfare make scant reference to CCI and vice versa.

ACKNOWLEDGMENT

This article is an expanded version of a paper presented at the 16th European Conference on Cyber Warfare and Security (Duvenage, Sithole & von Solms, 2017) and contains extracts from a doctoral thesis completed at the University of Johannesburg (Duvenage 2019)

REFERENCES

Bodmer, S. A. (2012). *Reverse deception–Organized cyber threat counter- exploitation.* New York: McGraw-Hill.

Heckman, K. E., Stech, F. J., Thomas, R. K., Schmoker, B., & Tsow, A. W. (2015) Cyber Denial, Deception and Counter-Deception: A Framework for Supporting Active Cyber Defense. Springer. doi:10.1007/978-3-319-25133-2

Duvenage, P. C. (2013). Counterintelligence. In H. Prunckun (Ed.), *Intelligence and Private Investigation: Developing Sophisticated Methods for Conducting Inquiries*. Springfield, IL: Charles C. Thomas.

Duvenage, P. C. (2019). *A Conceptual Framework for Cyber Counterintelligenc*e. Unpublished thesis, University of Johannesburg, Johannesburg.

Duvenage, P. C., & Hough, M. (2011). The conceptual structuring of the intelligence and the counterintelligence processes. Strategic Review for Southern Africa, 33(2).

Duvenage, P. C., Jaquire, V. J., & von Solms, S. H. (2019). A cyber counterintelligence matrix for outsmarting your adversaries. In *Proceedings of the 18th European Conference on Cyber Warfare and Security*. Academic Press.

Duvenage, P. C., Jaquire, V. J., & von Solms, S. H. (2019). A cyber counterintelligence matrix for outsmarting your adversaries. In *Proceedings of the 18th European Conference on Cyber Warfare and Security*. Academic Press.

Duvenage, P. C., Sithole, T. G., & von Solms, S. H. (2017). A conceptual framework for cyber counterintelligence – Theory that really matters! In *Proceedings of the 16th European Conference on Cyber Warfare and Security.* Academic Press.

Duvenage, P. C., & von Solms, S. H. (2013). The Case for Cyber Counterintelligence. In *Proceedings of the 5th International Workshop on ICT Uses In Warfare and Peace*. IEEE.

Duvenage, P. C. & von Solms. S.H. (2015). Cyber Counterintelligence: Back to the Future. *Journal of Information Warfare*, *13*(1).

Duvenage, P. C., Von Solms, S. H., & Corregedor, M. (2015). The Cyber Counterintelligence Process - a conceptual overview and theoretical proposition. In *Proceedings of the 14th European Conference on Cyber Warfare and Security*. Academic Press.

Duvenage, P. C., von Solms, S. H., & Jaquire, V. J. (2016). Conceptualising Cyber Counterintelligence – Two Tentative Building Blocks. In *Proceedings of the 15th European Conference on Cyber Warfare and Security*. Academic Press.

Gill, P. (2006). What is Intelligence Theory? In G.F. Treverton et al. (Eds.), *Toward a Theory of Intelligence – Workshop Report*. RAND. Retrieved from http://www.rand.org/pubi/larf/proceedings/2006Rand–CF219.pdf

Godson, R. (2001). *Dirty tricks or trump cards – U.S. covert action and counterintelligence*. New Brunswick: Transaction Publishers.

Greenwald, A. G. (2012). There is nothing so theoretical as a good method. *Perspectives on Psychological Science*, *7*(2), 99–108.

Jaquire, V. J. (2018). *A framework for a cyber counterintelligence maturity model*. Unpublished thesis, University of Johannesburg, Johannesburg.

Justiniano, J. E. (2017). *Advancing the capacity of a theater special operations command (TSOC) to counter hybrid warfare threats in the cyber gray zone*. Utica College.

Kaspersky. (2018). *State of Industrial Cybersecurity 2018*. Retrieved from https://usa.kaspersky.com/about/press-releases/2018_ics-cybersecurity

Lowenthal, M. M. (2012). *Intelligence: From Secrets to Policy* (5th ed.). Sage Publishers.

Oxford English Dictionary. (2016). Retrieved from http://0-www.oed.com.ujlink.uj.ac.za/view/Entry/74161?redirectedFrom=Framework

Panda Security Labs. (2018) *The hunter becomes the hunted: How cyber counterintelligence works*. Retrieved from https://www.pandasecurity.com/mediacenter/panda-security/cyber-counterintelligence/

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

Sims, J. E. (2009). Twenty-first-century counterintelligence. In J. E. Sims & B. Gerber (Eds.), *Vaults, mirrors and masks – Rediscovering U.S. counterintelligence*. Washington, D.C., US: Georgetown University Press.

Molander, R. C., Riddile, A., Wilson, P. A., & Williamson, S. (1996). Strategic Information Warfare - new face of war. RAND Cooperation Santa Monica.

Symantec. (2018). *Internet Security Threat Report Volume 23 - March 2018*. Retrieved from 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*. Retrieved from https://www.symantec.com/security-center/threat-report

The Economist. (2015). *Counter-intelligence techniques may help firms protect themselves against cyber-attacks*. Retrieved from http://www.economist.com/news/business/21662540-counter-intelligence-techniques-may-help-firms-protectthemselves