DOI:10.6531/JFS.201809_23(1).0006

Information Warfare as Future Weapon of Mass-disruption, Africa 2030s Scenarios[1]

Rianne van Vuuren
Institute for Futures Research
South Africa

Abstract

Information warfare is an emerging threat which is developing into a significant future global security challenge, especially as the relationship between information and power is strengthened. Futures studies generate foresight about the manifestation of information warfare in the 2030s as an upcoming national security threat in Africa. The four scenarios developed provide plausible futures which offer early warning insights on the manifestation of information warfare as a national security threat confronting Africa during the 2030s. Polarisation poses a significant future risk in terms of leveraging information warfare as a future weapon of mass-disruption.

Keywords: Information warfare, Cyber warfare, Netwar, Psychological operations, Futures studies, Environmental scanning, Foresight, Scenario study, 2030.

Introduction

In an age where information is increasingly positioned at the centre of society, a future in which information also becomes a security liability is a reality for Africa and the world at large. Information in all its manifestations – from data to wisdom – has been central to institutional power since the dawn of humankind. Technological efficacies brought about by the digital revolution and enhanced global networking activities have boosted the role of information in national power. Furthermore technological development catapulted information to the centre of most human endeavours, although high levels of inequality persist as manifested in the digital divide.

Information warfare is a subject intimately linked to the future because it is closely related to technology futures as well as the changing manifestation of warfare and conflict. Futures thinking is based on three interrelated inquiries into the future with the objective to create broad awareness about the future. The inquiries are measuring the future to obtain knowledge about the future; imagining the non-existing future; and purposefully designing or making the future. Measuring, imagining and making sustainable alternative futures should be the preferable outcome of holistic futures thinking and requires active interventions to realise (Spies, 2015). In this article, the focus is on the measuring and imagining dimensions, but it also provided insight regarding the design of countering information warfare futures in Africa by 2030[2]. Thus, a futurist perspective does not entail prediction of the future. Instead, the futurist strives to provide insight and foresight with the aim to promote knowledgeability which could assist in creating a preferable future.

The following key questions are focused on:

> *What is information warfare as well as its link to power?*
>
> *What are the main driving forces which will influence the shaping of the future of information warfare as a national security threat for Africa?*
>
> *What are the plausible scenarios in which information warfare would manifest as a national security threat for Africa?*
>
> *What propositions can be identified applying to the plausible information warfare threats against African governments and societies in the 2030s?*

Information and Power: the Growing Synergy and Implications for National Security

Before the scenarios, which the African population and governments could plausible be expected to be confronted by, could be presented, it is important to focus on what exactly constitute information warfare. Generally, the term information warfare is still associated with high-technology weapons and broadcast images of drones destroying military targets with apparently assured accuracy and computer hackers taking down a country's power grid by gaining control of the power supplier's mainframe computers. Unfortunately, this armchair view of the sometimes confusing capabilities made possible by high technology and information technology has created a simplistic and sanitised vision of information warfare in which, to paraphrase Toffler (1990), the mindless fist is replaced by the congealed mind.

The media's initial focus on guided missiles and intelligent warfare systems, the tangible element of the so-called digital battlespace, masked the potentially deeper societal implications of virtual warfare strategies and global power projection (Cronin & Crawford, 1999, p.257). Increasingly cyber security and cyber warfare are becoming a major threat narrative with a wide range of applications in the fields of crime, business and politics (Carr, 2012, pp.1-5). Of specific interest for further study is the additional intangible role that information and communication play in terms of success in this new unfolding conflict environment. It is suspected that this aspect might become a major determinant of potential future political and economic supremacy.

Information is increasingly linked to power. How a government uses that power progressively controls how effectively a country may be influencing world politics and national security. In the past, the elements of power included mainly military, economic and diplomatic factors. However, in the 21st century, information is rapidly assuming a key position in foreign and security policy. It can potentially fulfil many roles, such as being a force multiplier, a tool for influencing decision-making and/or an instrument for manipulation. Information has evolved into a significant power projection instrument for the state. However, as much as it presents an offensive power projection capability to the state, it also poses a potential momentous threat to the state and society in general (Armistead, 2004, p.231).

The constantly changing national security environment is linked to the shifting basis of state power. As the foundation of global civilisation evolved from agriculture to industry and then to the information sector, the power structures within states also changed. At its core, the transformation to an information-based society represents a shift from manufacturing to knowledge, where the creation, application and dissemination of knowledge, rather than the production of manufactured goods or agricultural products, is becoming the central defining activity of modern society and governance (Mazarr, 1997, p.25). This shift has a direct impact on how national security is being viewed by some governments. At the same time, there has been an increase in the number of countries studying innovative ways to endeavour to gain an advantage by changing the way in which conflict is managed and power is projected. The information society brings new and revolutionary technologies and means, which demand change in the way state security is managed (Lin, 2000). This has a broad impact on modern society, changing risk and threat analysis in most human endeavours.

Regardless of shifting global power structures, a coherent national security strategy is an important instrument for any state. All states, even those with limited resources, have a broad range of tools at their disposal to advance their interests. These tools, whether diplomatic, economic, informational or military, provide the means by which they seek to achieve their security objectives. A national security strategy provides a rational framework for specifying interests in a comprehensive and methodological way (Africa Centre for Strategic Studies, 2005, p.1).

While many governments have developed strategic security frameworks as national security strategies, this remains largely limited to the developed world countries. Even in the case of countries addressing information-related threats the focus remains largely limited to cyber security. However, the threat from the information environment is broader than the cyber dimension. The pervasiveness of information in modern society makes it a key factor in the construction of a global information society (Chadwick, 2006, p.209). The African Union's Agenda 2063 foresee a peaceful and secure Africa an integrated, prosperous and peaceful Africa, driven by its own citizens and representing a dynamic force in the international arena. (African Union Commission, 2015, pp.1-2).

Already in the 1990s the potential threat posed by information warfare was identified as a significant national security threat in the future (Waltz, 1998, p.13). A significant question to be asked is whether the information dimensions, especially in terms of their comprehensive implication for national security, are adequately addressed by an upcoming continental power such as Africa. Finding a practical definition for information warfare has been a challenge but a necessity for the development of information warfare futures in Africa by the 2030's.

Defining Information Warfare

While a significant amount of work has been done on efforts to define information warfare and related concepts, this is taking place mainly in the developed world. In general, information warfare has not been regarded in a comprehensive manner as a significant part of the national security threat perception in the developing world, especially in Africa. Larger developing countries such as China (Cheng, 2017, p.1) and India (Sekhar, 2015) are exceptions.

In this article the term information warfare is used in its contemporary and futurist contexts, but it is also acknowledged that the phenomenon has strong historical links. Although information warfare is a recent concept that has only been used since the early 1990s, diverse and sometimes even contradictory definitions of information warfare have complicated study of this phenomenon. Existing definitions of information warfare have limitations. These are related to being too expansive or purely focusing on USA military-centric definitions, and lastly being limited or largely limited to attacks on the ICT infrastructure and capacities of countries and/or entities (Arquilla & Ronfeldt, 2001; Denning, 1999; Ventre, 2009 & 2011).

While some aspects related to information warfare are as old as humankind, many aspects as to how it is being applied in our contemporary information driven world are new (Jones, Kovacich & Luzwick, 2002, p.5). In an effort to address the limitations of current definitions the following definition of information warfare is proposed: *Information warfare is defined as actions focused on destabilising or manipulating the core information networks of a state or entity in society with the aim to influence the ability and will to project power as well as efforts to counter similar attacks by an opposing entity and/or state* (van Vuuren, 2016, p.77).

The above definition encompasses three manifestations of information warfare, namely netwar, psychological operations and cyber warfare.

- Netwar is described by Arquilla and Rondfeldt (1997) as referring "… to an emerging mode of conflict at societal levels, involving measures short of traditional war, in which the protagonists use network forms of organization and related doctrines, strategies, and technologies attuned to the Information Age. These protagonists are likely to consist of dispersed small groups who communicate, coordinate, and conduct their campaigns in an internetted manner, without a precise central command."
- Cyber warfare (cyberwar) describes a power related conflict that takes place in cyberspace[3] (the virtual world and the internet) instead of in the physical world.
- Psychological operations refer to an intangible sphere, in essence the power related conflict area is people's minds, and criteria for winning or losing are also heavily culture-dependent (Eriksson, 1999, pp.57-64).

Taking into account the definition of information warfare as well as its constituent elements, information warfare is taking place on a cognitive-technological continuum. Within the cognitive sphere information warfare manifests as netwar and psychological operations. Within the technological sphere information warfare manifests as cyberwar. See Figure 1 for a graphical representation of the components of information warfare.

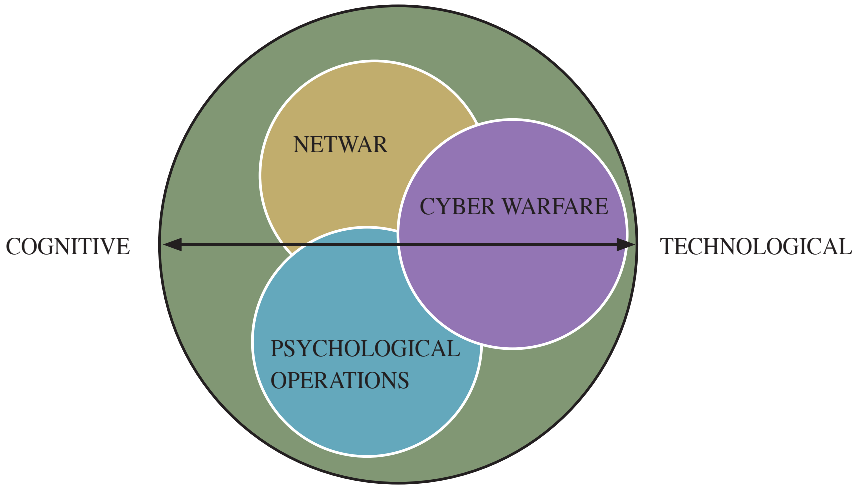


Figure 1. Components of information warfare

The Fundamentals of Information Warfare

Taking cognisance of information warfare as an overriding term, while also noting the history of information in conflict as well as criticism on existing definitions, the following fundamentals endeavour to identify some common elements as well as significant characteristics of information warfare:

- Information in especially a networking capacity is central to the information warfare concept with attaining information superiority as a tactical and strategic aim.

- Information warfare refers to the cognitive and technological disruption linked to conflict and war but not to the kinetic aspects associated with war and terrorist activities.
- Information warfare is linked to using information as instrument for manipulation, power projection, leveraging and creating an advantage.
- The strengthening of network-orientated organisations and interactions, while consequently hierarchical orientated organisations and interactions are weakened because of the information revolution and expansion of global communications (Arquilla & Ronfeldt, 2001, p.1).
- The global network ecology is transforming itself from a purely communications medium to a social environment of growing political and security significance (Vlahos, 1998, p.77).
- The exponential growth of technology, globalisation and increasing significance of networking are enhancing the future significance of information warfare.
- Information warfare is in essence a transdisciplinary concept covering a wide array of interests, including the political, governance, technological, psychological, social, media, economic and military fields.
- Both offensive and defensive roles are envisaged for information warfare.
- Information warfare is not bound by geographic limitations.
- The cost of conducting information warfare would in most cases be much lower compared to other forms of power projection.
- It is widespread and available to any country, and, in most cases, to any individual or group that wants it (McLendon, 1994). Technological skills barriers exist in the case of cyber warfare.
- The increasing dual-use nature of especially information technology results in many technologies having both military and civilian applications (Schneier, 2008).
- Information warfare invokes asymmetric action. Asymmetry is about the qualitative difference in the means, values and style of opposing powers. Once a state or entity insists on superiority in power projection, its disadvantaged opponents resort to unconventional asymmetrical means to oppose it, avoiding its strengths and concentrating on its vulnerabilities (Bishara, 2001).

The Future of Information Warfare

Taking into account the current manifestation of information warfare related issues (from Ransomware like WannaCry affecting hundreds of thousands of users to indications of international digital interference in national elections), governments worldwide are actively investigating and building information warfare capabilities. Most developed states and some developing states have conducted information warfare related exercises and established national monitoring entities (Breene, 2016). At the same time non-governmental entities are also getting involved in information warfare related activities (Cronin & Crawford, 1999, p.259). Information warfare is a global phenomenon, which makes it difficult if not impossible to evaluate in a domestic context. This will become even more so considering the future of information warfare.

Despite these capacities being created by governments and interest groups, the dynamics of emerging emergencies and the unintended consequences of information warfare make the control of information-driven dynamics highly problematic. Controlling the potential consequences of information war in terms of its netwar and psychological dimensions will be difficult, if not impossible, in the future. The emergence of various other information warfare actors other than government controlled entities remains a high probability in the future.

Protest movements and/or governments are massing force in the infosphere as well as cyberspace for viral propaganda and debilitating IT infrastructure attacks. As a result, there is a renewed focus on mass cyber-mobilisation and concentration as part of information warfare. Networked actions, cyber-mobilisation and rhizome[4] organisation are underpinning popular forms of conflict and not only lower impact cyber-related activities such as the disruption of websites. These activities require public participation for success and social media like viral organisations (Elkus, 2009).

In the future it can be expected that this form of mobilisation will even be more effective. The rise of artificial intelligence will probably change the nature of cyberwar in particular. Instead of relying on human hackers to carry out their attacks, antagonists will in the future continue to automate information warfare, relying on artificial intelligence systems to probe opposing defences, carry out attacks, and defend against opponents' artificial intelligence. It is probable that this competition could eventually outstrip human control or even monitoring (Pazvakavambwa, 2018).

In the modern field of struggle between a sovereign country and non-state actors it also becomes necessary to refer to the information warfare that is taking place in the new and traditional media as well as other technological platforms, from the internet to virtual reality and computer games. Such groups, including terrorist organisations, continue to invest efforts in information warfare tools, which enable them to bridge the physical gap between these entities and their conventional law enforcement and security forces. Some of these entities' irregular capacities will probably outstrip the competencies of states in this regard (Gilat, 2009).

These largely asymmetric warfare capabilities, which include information warfare, are even empowering the individual to conduct war. While the concept of asymmetric warfare dates back to ancient times, most modern conflicts have redefined the nature of such struggles. As the manifestation of information warfare indicates, warfare is being transformed from a closed, state-sponsored affair to one where the means and know-how to do battle are readily found on the internet and social networks. This open and global access to increasingly powerful technological tools is in effect allowing small groups to declare war on states. Insurgent groups can be expected to increasingly form loose and non-hierarchical networks to pursue a common vision. United by that vision, they exchange information and work collaboratively on tasks of mutual interest (Charette, 2007).

Outcome of an Environmental Scan

In measuring and imagining the future of information warfare for Africa an environmental scan was used to evaluate the current milieu within which information warfare manifests with the capacity to also provide some level of insight into the driving forces which will influence how it might manifest in the future. The environmental scan focused on events, developments and manifestations related to information warfare and national security within the Technological, War/Conflict, Economical, Political and Social (TWEPS) macro-environmental hexagon, which is used instead of the frequently used STEEP (Social, Technological, Economic, Environmental and Political) sectors[5] (Kurian & Molitor, 1996, p.814). This multi-disciplinary environmental scanning focused on literature with the aim to identify current manifestations and to recognise possible trends and driving forces flowing from this (van Vuuren, 2016, p.77). See Figure 2 (Adapted from Spies, 2005) for a graphical representation of the TWEPS macro-environmental hexagon.

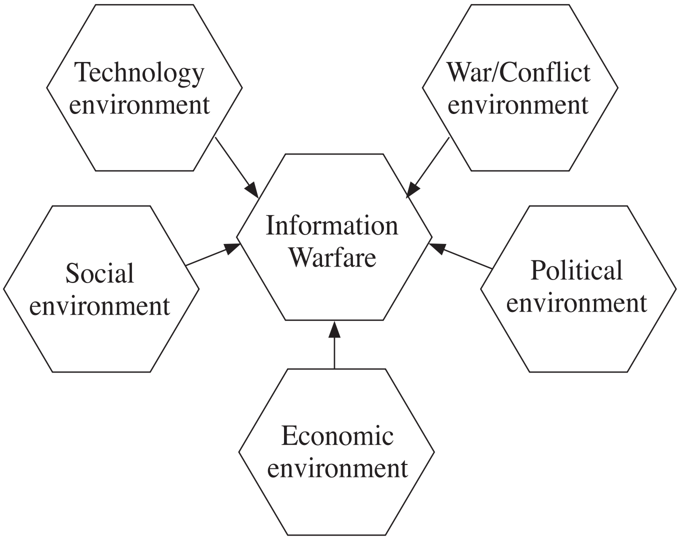


Figure 2. The TWEPS macro-environmental hexagon

The outcome of the environmental scan focusses on three overriding trends present in all environments. Transformation, networking and the impact of technological innovation in all the environments investigated were highlighted as central to the manifestation of information warfare currently as well as in the future. These trends influence not only the entities involved in power relations in society, but also enhance the potential influence and power of small and marginalised entities in society. New forms of network-related actions such as the rhizome phenomenon (small, highly interconnected networks) using social network phenomena for cyber mobilisation have been identified as of particular use for information warfare in the future. In order for information warfare activities in line with the identified trends to accomplish any outcome it should be focused on specific targets in the information society.

Information warfare targets are multi-dimensional, focusing on tactical and strategic targets. The environmental scan highlighted the significance of growing interdependence and globalisation in economic prosperity, exposing the commercial networks and the global service sector as highly vulnerable to all constituent elements of information warfare, namely netwar, cyberwar and information operations. Information warfare is primary targeted at the power structures in any state. These structures are part of the complex and inter-related processes and services underlying the information structures in society. In this regard, see Figure 3 for an illustration of the pillars of an information society. The key vulnerable access points include factors underlining the networking, coordination, integration, compatibility and connectivity of the information and knowledge society.

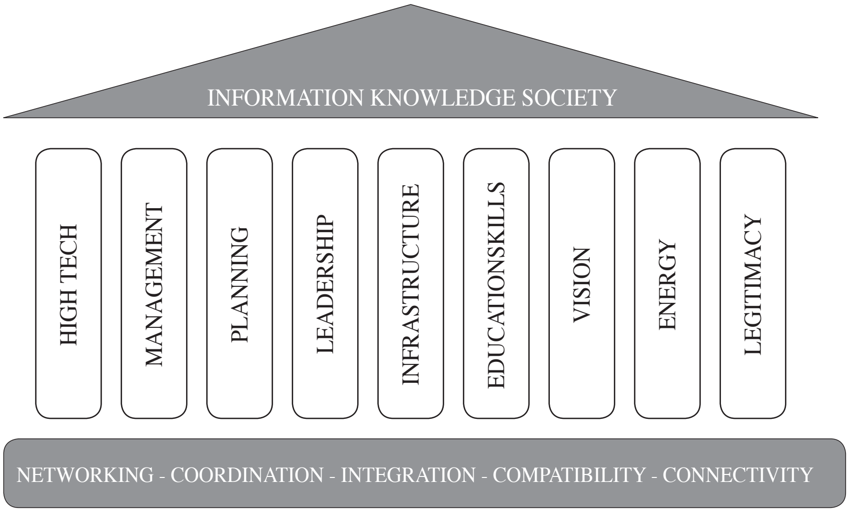

INFORMATION KNOWLEDGE SOCIETY
HIGH TECH
MANAGEMENT
PLANNING
LEADERSHIP
INFRASTRUCTURE
EDUCATIONSKILLS
VISION
ENERGY
LEGITIMACY
NETWORKING - COORDINATION - INTEGRATION - COMPATIBILITY - CONNECTIVITY

Figure 3. The pillars of an information society

Based on an evaluation of the past manifestation of information warfare, it can be concluded that practically all recent conflict situations have had an information dimension (van Vuuren, 2016, pp.116-124). While information warfare enhances military power, especially in developing countries, it also creates new vulnerabilities. It can be assumed that this trend will continue and that nearly all future conflict situations will have an information warfare dimension.

Social media and internet/mobile device platforms for such media empower most net-enabled individuals with an interest in participating in practically any global issue (van Vuuren, 2016, p. 262). This has created platforms for involvement and participation in social and political issues on a level never seen before in the history of humankind. Increasingly, it does not matter what the majority's view on issues are; it matters more what the majority of "empowered individuals" are doing.

Identification of the Scenario Drivers

The process to identify the scenario drivers is done by using qualitative text analysis on the outcome of the environmental scan deploying coding techniques, assisted by the use of software. Coding can be done using structured or unstructured data as source material. The best results are obtained by using qualitative text analysis of documentary source material (Kuckartz, 2015).

Kuckartz (2014, p.33) states that qualitative text analysis is a form of analysis in which an understanding and interpretation of the text play a far greater role than in classical content analysis, which is more limited to the so-called manifest content. In qualitative text analysis, codes are typically words or devices used to identify themes. As the research focuses on theme-related issues associated with the current and future manifestation of information warfare, thematic qualitative text analysis is focused on the environmental scan's text in its entirety, identifying the common occurring codes.

After studying the text, the summative, essence-capturing codes are identified, which are applicable to all text in the environmental scan narrative. Three such overarching codes have been identified. The three coding concepts overlap to some extent but for each paragraph the essence-capturing categories and then subcategories are conceptualised. The source of these qualitative text analysis thematic coded categories, identified as Innovation, Networks and Transformation, is the three cross-cutting trends identified from the environmental scan.

Firstly, the rapid spread of technology and innovation has a major impact on states, organisations and individuals while also contributing to significant inequality. Secondly, the world community has reached a new level of integration, accompanied by the rise of networks, especially social networks. Thirdly, societal change has been accelerated to new levels, resulting in transformation as a constant reality affecting nearly all social entities. The outcome of the environmental scan is coded using Coding Analysis Toolkit (CAT) software developed by the University of Pittsburgh's Qualitative Data Analysis Program (QDAP) (University of Pittsburgh, 2015).

The value of the identified driving forces is increased when the driving forces are scrutinised, integrated, prioritised and validated by panels of global and local experts knowledgeable about information within the TWEPS environments. For this purpose two Delphi studies are conducted as the most appropriate method for arriving at an expert validation and consensus on the key driving forces impacting the manifestation of information warfare as a national security threat by the 2030s.

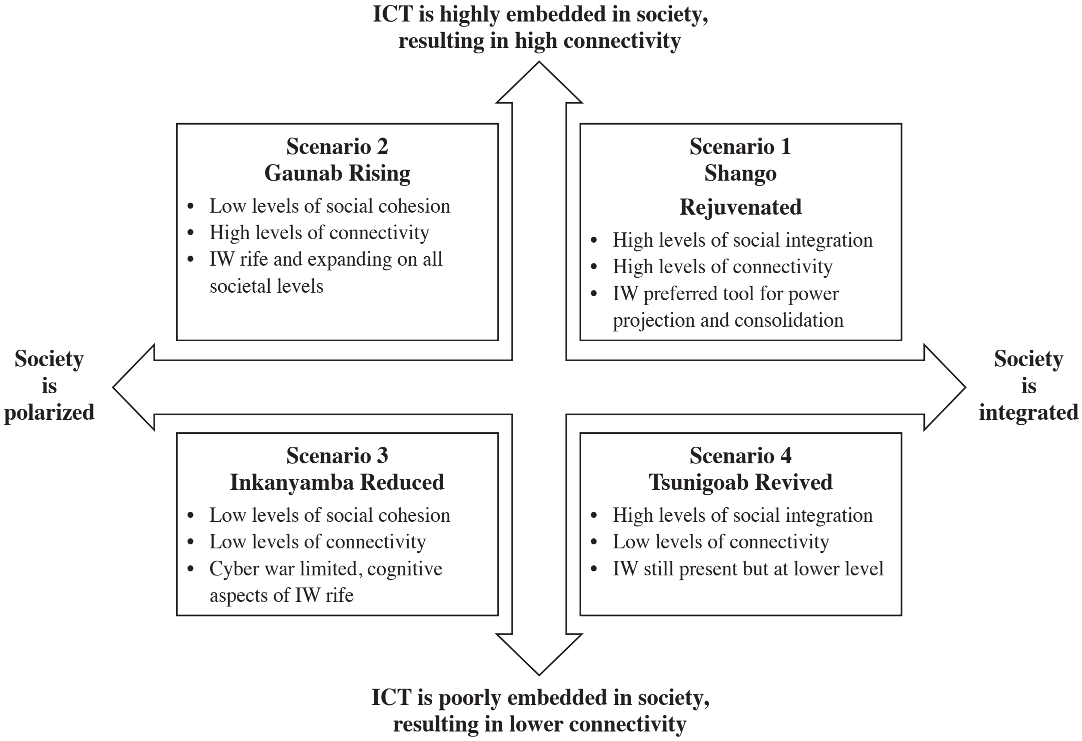
Two separate Delphi studies were conducted. The one Delphi study used South African security experts while the second Delphi study uses both domestic and international experts (knowledgeable in one or more TWEPS environments). Input from a multi-disciplinary pool of experts enhanced the value of the analysis already done during the environmental scan and also provided some additional input and insight to the development of scenarios.

The two Delphi studies refined and validated the ten most significant drivers influencing the manifestation of information warfare as a national security threat in the 2030s:

- The centre of power is shifting from the traditional developed countries to the developing countries.
- Security in a networked environment will increase in complexity as its physical and non-physical elements become more tightly interwoven.
- An increase in integration and polarisation will contribute to systemic stresses.
- Information warfare will become a growing option for power projection.
- Symbolic, information-related phenomena are increasingly impacting behaviour.
- The speed of change is increasing exponentially with global communication becoming instantaneous.
- Non-state actors are increasing their influence related to global security.
- Global and intra-regional inequalities are stimulating conflict potential.
- Information communication technology (ICT) is embedding itself as a crucial part of society.
- Social media is a significant part of communication and this is expected to grow in the future.
- The two most significant driving forces for scenario building are obtained by combining the prioritisation of the Delphi studies creating the two key drivers namely:
- An increase in integration and polarisation will contribute to systemic stresses.
- ICT is embedding itself as a crucial part of society.

Africa Information Warfare Scenarios 2030s

The horizontal axis of the scenario matrix represented the spectrum measuring the extent to which ICT is embedding itself as a crucial part of society. The upper side of this spectrum represented an environment in which ICT is highly embedded in society resulting in high connectivity. The lower side of the axis represented an environment in which ICT is poorly embedded in society resulting in lower connectivity. The vertical axis represented a spectrum measuring the extent to which integration and polarisation will contribute to societal systemic stresses. The right-hand side of this axis represented an environment in which society experiences high levels of integration. The left-hand side of this axis represented an environment in which society experiences high levels of polarisation. Thereby four information warfare scenarios for Africa in the 2030s are created (See Figure 4).



ICT is highly embedded in society, resulting in high connectivity

Scenario 2
Gaunab Rising
- Low levels of social cohesion
- High levels of connectivity
- IW rife and expanding on all societal levels

Scenario 1
Shango
Rejuvenated
- High levels of social integration
- High levels of connectivity
- IW preferred tool for power projection and consolidation

Society is polarized

Society is integrated

Scenario 3
Inkanyamba Reduced
- Low levels of social cohesion
- Low levels of connectivity
- Cyber war limited, cognitive aspects of IW rife

Scenario 4
Tsunigoab Revived
- High levels of social integration
- Low levels of connectivity
- IW still present but at lower level

ICT is poorly embedded in society, resulting in lower connectivity

Figure 4. Information warfare 2030s scenarios

Rationale for the scenario names

Metaphors from African traditional religion and myth are adopted for the identified scenarios with the aim to advance creative thinking about the content of the scenarios and setting it within an Africa milieu.

Shango is from Yoruba tradition in Nigeria. As an earth deity he was once a mortal man, the king of Oyo, who transformed himself into an immortal. According to tradition, during his life he breathed tongues of fire. He then ascended into the sky by climbing a golden chain and became the god of thunder and lightning. He is also god of justice, punishing thieves and liars (Jordan, 2004, p.282). Shango Rejuvenated illustrates a scenario in which a high level of ICT embeddedness and high levels of integration boost assimilation, cooperation and technological advancement but also provide the ideal staging area for the use of information warfare as power projection method.

Gaunab is malevolent god of darkness from the Khoi culture in Namibia. This deity is the chief adversary of the creator god Tsunigoab. He was engaged in a primordial struggle for supremacy during which Tsunigoab was wounded but eventually triumphed, consigning Gaunab to the so-called "dark heaven" (Jordan, 2004, pp.102-103). Gaunab Rising does not necessarily reflect the rise of authoritarian societies but rather highlights the possible consequences of international, regional and even national polarisation in an environment in which high levels of ICT embeddedness will enhance the capabilities of all the role-players involved in society.

Inkanyamba is a Zulu storm god from South Africa. The deity is specifically responsible for tornados and perceived as a huge snake coiling down from heaven to earth (Jordan, 2004, p.139).

Inkanyamba Reduced reflects a polarised environment in which the embeddedness of ICT remains at a low level. Although the technological element of information warfare such as cyberwar could be constrained, high levels of potential conflict are experienced.

Tsunigoab is the creator god in the Khoi tradition in Namibia. Tsunigoab walks with a limp, because of an injury sustained in a primordial battle with his arch rival Gaunab, the god of darkness, who was eventually driven away to live in the dark heaven. Tsunigoab is invoked at dawn each day (Jordan, 2004, p.323). Tsunigoab Revived reflects a scenario in which a high level of social, political and economic integration is achieved but this is not supported by a high level of ICT embeddedness in society overall, resulting in general stability but difficulty in maximising technological opportunities in society.

Scenario 1: “Shango Rejuvenated”

The first scenario is one in which technological progress takes place in an increasingly cooperative and networked global society. This scenario is formed in the quadrant where both the two main driving forces – ICT embeddedness and societal integration – are high. This provides for a highly technological driven African society in which the consumer and business demand for technological solutions are elevated. Information warfare is seen as a common but also practical and useful instrument for the projection of power by many entities within Africa. In Africa the governments and other prominent local and international role-players are forcing commercial values on the continent, creating a largely homogeneous landscape, with main stream diversity decreasing and some sub-cultures forced to the margins. Information warfare is regarded by many domestic but also foreign role-players as a legitimate method for dissent and conflict. The governments but even larger corporate entities invest significant resources into both defensive and offensive capabilities.

Shango Rejuvenated: Information Warfare and National Security Manifestation

The high levels of social cohesion play a role in limiting both international as well as domestic conflict and war. However, competition, especially competition leading to conflict, remains common. Because of the high level of ICT embeddedness in African society, information warfare remains a useful as well as viable instrument of influence and power projection. Many African states continue to survive challenges against their legitimacy. However, powerful non-state entities such as corporations and ideological or religious groups continue to challenge the sovereignty of many African states.

As interconnected high technology and especially the digital economy are central to stability and wealth creation in Africa, societies are highly vulnerable to information warfare. It also occurs on all levels and in all of its manifestations as cyberwar, netwar and psychological operations. Information warfare is regarded as a major national security issue in most African states. It is also being developed by some governments and other entities as offensive power projection tools. At the same time counter measures against threats are highly specialised and evolving fast. Networked security is seen in Africa as of major significance and substantial resources are invested in this.

The relevance of information warfare is strengthened by the systemic nature of conflict because of the high levels of ICT embeddedness. Conflict is highly complex with growing interaction between technological change, system development and operational innovation. Within Africa the deployment of autonomous weapons and security systems are common. Asymmetric action forms part of conflict in Africa but is somewhat restrained because of high levels of global integration and the focus on multi-level defensive capabilities.

Africa’s multi-lateral security cooperation is strengthened and assists in the overall maintenance of order in the international system. Africa is exposed to less inter-state conflict while the occurrence of intra-state conflict within the countries is increasing in which information warfare will increasingly become the method of choice for dissent. The added value of high level anonymity provided by technology, especially with cyberwar, is also exploited by non-government institutions and the government alike. Globally the borders between military and civilian conflict weakens partly because of the proliferation of power projection opportunities brought about by information warfare options. This leads to the expansion of a technological arms race between governments and non-government groups. Despite the information warfare related challenges in general, a balance of power within Africa as well as between African countries and foreign competitors in terms of this phenomenon exists as counter measures are largely in place or are developed quickly.

Terrorism presents a threat in Africa but increases also in the non-physical (information warfare) part thereof. Crime and terrorism are increasingly being combated by way of algorithms and big data. In Africa crime and terrorism groups use advanced technology that is basically matched by the advanced technology of the government entities opposing them. The high levels of integration in Africa will also result in the expansion of the reach and innovativeness of disruptive and terrorist means.

Scenario 2: "Gaunab Rising"

The second scenario is one in which technological progress takes place in an increasingly polarised society. This scenario is formed in the quadrant where the two main driving forces – ICT embedding and polarisation – are high. While technological progress and technological interconnectedness are high, the potential thereof cannot be realised because of divisions in society. This scenario represents a divisive continent with increasing competition between societies mobilised on the grounds of status, nationality, religion and class, providing opportunities for authoritarian elites to expand control. Information warfare remains rife and its use is expanding on all societal levels. Inequality of capacities could lead to rapidly changing power configurations.

Gaunab Rising: Information Warfare and National Security Manifestation

The nation state is paramount, but non-state entities organised on religious, ideological and national grounds do present a growing threat to national security. Full-blown information conflicts and wars are common with a mix of kinetic and non-kinetic elements. In this regard virtual cyber-based groups such as Anonymous (or its future successors) pose a major national security threat. Non-state actors regard information warfare as a primary tool to promote and advance their political agendas.

In Africa information warfare thus poses a significant national security risk and growing ICT embeddedness ensures that states are highly vulnerable, especially to cyberwar. The level of potential hostility in Africa ensures that all methods for promoting interests in a fairly hostile environment are used. Both terrorism and cybercrime are serious local and global threats. Information warfare is regarded as a legitimate instrument of power projection by both the elite and the dissatisfied in Africa. The ruling elites in African countries manipulate and force the rest of the population into submission with whatever means at their disposal. However, the marginalised are also turning to information warfare as a practical tool to pursue their interests. Conflict becomes highly complex and common with growing interaction between technological change, system development and operational innovation. Asymmetric war and conflict options are an ingrained part of conflict and war globally.

The broader continental and global environment experience an increase in inter-state and intra-state conflict. The threat of nuclear war will be significant as the non-proliferation system is increasingly eroded. The start of a Second Cold War is a potential risk, especially if authoritarian states expand their assertive stands and military capabilities. This leads to an escalation of an arms race with high-technology weapons and even weapons of mass destruction (WMD). Private armies (mercenaries) are significant role-players in these conflicts. Drone warfare is rife and used by many governments and even non-government role-players.

Scenario 3: "Inkanyamba Reduced"

The third scenario is one in which polarisation is high while technology participation is low. This scenario is formed in the quadrant where the ICT embedding is low but polarisation is high; magnifying dissent, resulting in high levels of conflict and competition for resources. The technological part of information warfare in the form of cyberwar is limited, but the cognitive aspects in the form of netwar and psychological operations remain high. Elites control resources and inequality is widespread.

Inkanyamba Reduced: Information Warfare and National Security Manifestation

The potential for general anarchy is a significant national security risk resulting in security being a major but also expensive reality in African countries as well as in many other countries. In most cases, only the wealthy in Africa can afford security. The use of information warfare (especially netwar and psychological operations) is widespread. In general, the mix of kinetic and non-kinetic elements in war and conflict is common. Asymmetric war and conflict options form an ingrained part of conflict and war globally, although it is not as technology driven as it could be. Inequality leads to conflict and unrest in many African countries. Conflict about resources is common and hybrid warfare is widespread worldwide. The global non-proliferation system collapses and increases the possible use of WMD substantially. An arms race between states and even in some cases non-state entities are a reality.

The nation state including African countries are under pressure as non-state entities organised on religious and ideological foundations assert alternative and hybrid configurations. Ultra-regulated digital and physical fortresses are maintained in Africa, while outside of these a general "survival of the fittest" mind-set reigns. Private armies (mercenaries) are significant role-players in security as well as in the conduct of conflict.

Scenario 4: "Tsunigoab Revived"

High levels of social integration with low levels of technological participation ensure relative stability but also limit the potential value that technology could add to society. This scenario is formed in the quadrant where societal integration is high and ICT embeddedness is low. Levels of information warfare are lower but information warfare continues to be an instrument for power enhancement in society. Inequality continues to be a challenge.

Tsunigoab Revived: Information Warfare and National Security Manifestation

African governments remain paramount while non-state entities organised on religious, ideological and ethnic grounds do present some level of threat to national security. Information war is part of the power projection instruments available to state and non-state role-players. Cyber warfare's significance, however, is diminished by the lack of ICT embeddedness in society. Asymmetric threats and operations form part of conflict but are restrained because of high levels of global integration. These threats and operations are disruptive when they occur. The threats associated with global conflict types, such as nuclear war, are less significant as the multi-lateral system is more robust as a result of the high levels of international cooperation that are maintained. Global and national conflict continues but the risk of serious escalation is lower. The start of a new global Cold War is unlikely. Terrorism remains a threat but counter measures are more coordinated in this more cooperative global environment.

Propositions

The formulation of the propositions is done from the viewpoint of endeavouring to find commonalities between the different information warfare scenarios. Although the propositions focus on African situations similar to the scenarios, the perspective is applicable globally. Information warfare as national security threat is so ingrained in global society that it is difficult to only restrict these propositions to Africa.

- *Information warfare will be a national security threat of note by the 2030s.*
- *Multi-lateral measures would be ineffective to control information warfare.*
- *Polarisation poses a significant risk for the boosting of information warfare as a national security threat.*
- *Innovative forms of network-related actions will transform information warfare into ever-changing manifestations in the national security threat environment.*
- *While information warfare is a national security threat, it also potentially implies an information warfare threat from the state posed to the freedom of the population.*
- *Information warfare will become ingrained in society as the virtual and real worlds increasingly merge.*
- *The identified four information warfare scenarios for the 2030s as well as the information warfare future model can serve as frameworks or mental models for wider application in the TWEPS environments and further research.*

Conclusion

Globalisation and a high level of interconnectedness are changing the world, creating new national security challenges, processes and actors. Despite optimism that multi-lateral efforts would solve global security problems, it is clear that significant work still needs to be done in this regard. In terms of containing information warfare, it is even seriously questioned if any multilateral agreement to contain this phenomenon would even be possible, as verification would be practically impossible. It can be expected that national security will remain a national government responsibility, albeit a much more complex phenomenon in which individuals, non-state actors and alliances of individuals and other entities will be highly relevant actors. It can be expected that with technological development will come many innovations and improvements in the quality of life. At the same time, the negative side of these technologies will also be present and will mutate to hamper the development of solutions.

The two key driving forces on the continuum presented by the level of integration versus polarisation and the level of ICT embedding in society will be crucial in the manifestation of information warfare by the 2030s. On a strategic level, the management of these two driving forces and the countering of polarisation will be crucial in negating the threats posed by information warfare. However, irrespective of which scenario manifests, information warfare will become a national security threat of note by the 2030s. As economic, political and social life becomes more and more intertwined in everyday life, so does the vulnerability of humankind.

Furthermore the plausible scenarios also highlights how countries are able to manage discontent through a collaborative ethic of common purpose namely the ability of countries to build and sustain partnerships to combat discontent will increasingly depend on bolstering a country's credibility with the broader global population and forging an ethic of common purpose. It can be expected that political credibility and international esteem will probably grow in political significance in the future. The Western model of political development and values was dominant up to the 20th century but is increasingly being challenged by the rise of Asia and Africa. The political democratic models as conceived and developed by the West will not necessary represent the models for the political environment of the future.

The threat of some form of global anarchy is an underlying theme regarding the nexus of the identified main driving forces namely polarisation and ICT embeddedness in the future. Therefore the importance of strengthening national and social will to enhance collaboration and shared common purpose might be that which will differentiate places of human progress from places of increasing inequality and increased chaos in the future.

The viability of futures research is related to the quality of the research methods used. The viability of futures research is also associated with the diversity of research methods used, specifically in the developing world. As long as futures research is seen as a sole domain of the developed North, it will struggle to maintain its global position as an instrument of change and sustainable growth.

Correspondence

Rianne van Vuuren
Research Associate
Institute for Futures Research
South Africa
E-mail: riannevanvuuren@gmail.com

Endnotes

1. This article is based on research conducted for a University of Stellenbosch (US) Futures Study PhD thesis: "Information warfare as future South African national security threat" finalized in 2016.
2. In this article, the 2030s are set as the timeframe for the development of scenarios because of various reasons. As this study was conducted during the period from 2008 to 2015, the 2030s provides a time horizon of minimum 15 years, which is short enough to fit comfortably in the lifespan of individuals involved and interested in the question of how information warfare might influence society, but long enough to feel confident that significant changes in this regard could occur over this time period. At the same time, South Africa's National Development Plan (NDP) 2030, drafted in August 2012 by the National Planning Commission (2011), contains a series of proposals to eliminate poverty and reduce inequality by 2030.
3. Arquilla and Ronfeldt (1997, p.41) described cyberspace as follows: "… is a bioelectronic environment that is literally universal, it exist everywhere where there are telephone wires, coaxial cables, fibre-optic lines or electro-magnetic waves. This environment is inhabited by knowledge, existing in electronic form." Cyberspace consists of two measurable elements: connectivity and content. Connectivity encompasses the physical hardware, software and connecting electromagnetic or cable media that permit the generation, transfer, storage and sharing of data. The second element of cyberspace is content which influences behaviour and decision-making (Campen, 2008).
4. Deleuze and Guattari (1980, p.29) used rhizome as a metaphor to refer to a non-hierarchal form of organisation. Vail (2007) has extended this metaphor, referring to rhizome as an alternative mode of human organisation consisting of a network of minimally self-sufficient nodes that leverage non-hierarchal coordination of economic activity. The two key concepts of rhizome are self-sufficiency, which eliminates the dependencies that characterise hierarchy, and loose but dynamic networking that uses the "small worlds" theory of network information processing to allow rhizome networks to overcome information processing burdens typical of hierarchies. Rhizome therefore refers to an organisational pattern characterised by interconnected but independent networks of entities.

5. As the focus of research is on information warfare, the applicability of the STEEP sectors would need to be critically evaluated. Haberman (2013) identifies the Environmental (Ecology) Scanning sector as encompassing the natural world around us and understanding how the nature affects humanity and how humanity affects nature. Issues of concern are inter alia global warming, clean water, air quality, agriculture and increasing severity of storms. While these phenomena do have a significant influence on the world currently and in the future, these phenomena do not significantly manifest in the information warfare domain. Additionally the absence of the phenomena such as war and conflict, which go to the core role of information warfare in society as an additional fully-fledged sector, can be regarded as a significant gap. Therefore, the environmental sector is replaced with a War/Conflict sector creating the Technological, War/Conflict, Economic, Political and Social (TWEPS) macro-environmental hexagon.

References

Africa Centre for Strategic Studies. (2005). *Background paper on the senior leader seminar*. Gaborone, Botswana, 19 June to 1 July.

African Union Commission. (2015, April). *Agenda 2063: The Africa we want*. Final Edition.

Armistead, Edwin. L. (2004). *Information operations: Warfare and the hard reality of soft power.* Washington DC: Brassey's.

Arquilla, John., & Ronfeldt, David. (1997). Information, power and grand strategy. In Arquilla, John. & Ronfeldt, David. (Eds.), *Athena's camp: Preparing for conflict in the information age*. Santa Monica: RAND Corporation, MR-880. Retrieved April 15, 2005, from http://www.rand.org/publications/MR/MR880/indext.html

Arquilla, John., & Ronfeldt, David. (2001). The advent of netwar (Revisited). In Arquilla, John. & Ronfeldt, David. (Eds.), *Networks and netwars: the future of terror, crime, and militancy.* Santa Monica: National Defence Research Institute, RAND.

Bishara, Marwan. (2001, October 3). An enemy with no forwarding address. *Le Monde Diplomatique*, Retrieved January 12, 2004, from ttp://mondediplo.com/2001/10/03asymmetry

Breene, Keith. (2016, May 4). Who are the cyberwar superpowers? World Economic Forum. Retrieved April 8, 2018, from https://www.weforum.org/agenda/2016/05/who-are-the-cyber-war-superpowers/

Campen, Alan. D. (2008, January). Cyberwar, anyone? *SIGNAL Magazine*. Retrieved January 8, 2008, from http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=1452&zoneid=223

Carr, Jeffrey. (2012). *Inside cyber warfare*. Sebastropol: O'Reilly Media.

Chadwick, Andrew. (2006). *Internet politics: States, citizens, and new communication technologies*. Oxford: Oxford University Press.

Charette, Robert. N. (2007, November). Open-source warfare. *IEEE Spectrum*. Retrieved December 15, 2007, from http://blogs.spectrum.ieee.org/riskfactor

Cheng, Dean. (2017). *Cyber dragon: Inside China's information warfare and cyber operations*. Santa Barbara: Praeger.

Cronin, Blaise., & Crawford, Holly. (1999). Information warfare: Its application in military and civilian contexts. *The Information Society*, 15(4), 257-263.

Deleuze, Gilles., & Guattari, Félix. (1980). *A thousand plateaus: Capitalism and schizophrenia*. London and New York: Continuum.

Denning, Dorothy. E. (1999). *Information warfare and security*. Reading MA: Addison-Wesley.

Elkus, Adam. (2009). The rise of cyber-mobilization. *Groupintel.com*. Retrieved February 16, 2009 from http://www.groupintel.com/2009/02/13/the-rise-of-cyber-mobilization

Eriksson, E. Anders. (1999). Viewpoint: Information Warfare: Hype or Reality? *The Nonproliferation Review*, Spring-Summer, 57-64.

Gilat, Amir. (2009). Information warfare in the 21st century: Ideas are sometimes stronger than bombs. *Eurekalert.org*. Retrieved March 23, 2009 from http://www.eurekalert.org/pub_releases/2009-03/uoh-iwi031809.php.

Haberman, Michael. (2013, April). Four ways to do environmental scanning. *Omega Solutions Blog*, Retrieved July 25, 2016 from http://omegahrsolutions.com/2013/04/four-ways-to-do-environmental-scanning.html

Jones, Andrew., Kovacich, Gerald. L., & Luzwick, Perry. G. (2002). *Global information warfare: How businesses, governments, and others achieve and attain competitive advantages*. Boca Raton: Auerback Publications.

Jordan, Michael. (2004). *Dictionary of Gods and Goddesses* (2nd edition). New York: Facts On File, Inc.

Kuckartz, Udo. (2014). *Qualitative text analysis: A guide to methods, practice and using software*. London: Sage.

Kuckartz, Udo. (2015, April 3). Personal e-mail communication responding to question on the use of documentary material in qualitative text analysis.

Kurian, George. T. & Molitor, Graham. T. T. (1996). *Encyclopaedia of the future*, Volume 2. New York: Simon and Schuster Macmillan.

Lin, Abe. C. (2000). Comparison of the Information Warfare Capabilities of the ROC and PRC. *Cryptome*. Retrieved October 27, 2005 from http://cryptome.org/cn2-infowar.htm

Mazarr, J. Michael. (1997). *Global trends 2005: The challenge of the new millennium*. Cambridge, MA: Center for International Studies.

McLendon, James. W. (1994, April). Information Warfare: Impacts and Concerns. *Air War College Maxwell Air Force Base.*. Retrieved March 2, 2008, from http://warandgame.wordpress.com/2008/02/24/information-warfare-impacts-and-concerns/

National Planning Commission. (2011). *National development plan: Vision for 2030*. Pretoria: South African Government.

Pazvakavambwa, Regina. (2018, March 1). AI now on cyber criminals' agenda. *ITWeb*. Retrieved on April, 8, 2018 from https://www.itweb.co.za/content/G98YdMLxaapMX2PD

Schneier, Bruce. (2008, May 1). America's Dilemma: Close Security Holes, or Exploit Them Ourselves. *Wired News*. Retrieved May 4, 2008. from http://www.wired.com/politics/security/commentary/securitymatters/2008/05/blog_securitymatters_0501

Sekhar, Raja. (2015). Digital India in the age of information warfare. *GreatGameIndia Magazine*, Oct-Dec 2015 issue. Retrieved March, 6, 2018 from http://greatgameindia.com/digital-india-in-the-age-of-information-warfare/

Spies, Phillip. (2005). Measuring and making the future. Volume 4: The views of futurists. In Slaughter, Richard. A. (Ed.), *Knowledge base of future studies*. Foresight International, CD-ROM.

Spies, Phillip. (2015). Futures Studies' 'Holy Trinity' within the context of a trained futures mind. Stellenbosch: Institute for Futures Research, Stellenbosch University. *Learning Hub Lecture Notes, Principles of Futures Studies*.

Toffler, Alvin. (1990). *Powershift, knowledge, wealth and violence at the edge of the 21st century*. London: Bantam.

University of Pittsburgh. 2015. *Coding Analysis Toolkit (CAT). Qualitative Data Analysis Program (QDAP)*. Retrieved and used for coding May, 18 to 20, 2015 from http://cat.ucsur.pitt.edu/app/main.aspx

Vail, Jeff. (2007). What is rhizome? Retrieved December, 5, 2008 from http://www.jeffvail.net/2007/01/what-is-rhizome.html

Van Vuuren, Rianne. (2016). *Information warfare as future South African national security threat*. PhD thesis. Stellenbosch: Stellenbosch University.

Ventre. Daniel. (Ed). (2011). *Cyberwar and information warfare*. London: ISTE Ltd & John Wiley and Son Inc.

Ventre, Daniel. 2009. *Information warfare*. London: ISTE Ltd & John Wiley and Son Inc.

Vlahos, Michael. (1998). The emergence of the infosphere and its impact on military operations. In Campen, Alan. D. & Dearth. Douglas. H. (Eds.), *Cyberwar 2.0: Myths, Mysteries and Reality*. Fairfax: AFCEA International Press.

Waltz, Edward. (1998), *Information warfare: Principles and operations*. Boston: Artech House.