RELEVANCE OF INFORMATION WARFARE MODELS TO CRITICAL INFRASTRUCTURE PROTECTION

Brett van Niekerk and Manoj S. Maharaj
School of Information Systems and Technology, University of KwaZulu-Natal

Abstract

This article illustrates the relevance of information warfare models to critical infrastructure protection. Analogies of information warfare models to those of information security and information systems were used to deconstruct the models into their fundamental components and this will be discussed. The models were applied to critical infrastructures to illustrate the relevance to critical infrastructure protection. By considering the interdependencies of the critical infrastructure sectors, it will be shown how all critical infrastructures can be modelled as information infrastructures when considering information warfare attacks.

Introduction

Information warfare first gained prominence in the early 1990s, and is still a developing concept.[1] As such, there is no standard definition of information warfare; however, at a basic level, information warfare is concerned with attacking and defending information and the infrastructure that supports it. Due to the interdependencies of critical infrastructure sectors on each other, an attack on one sector may result in secondary effects on other sectors. Of particular interest is the possibility of using the information and communications sector to launch attacks on other sectors. Critical infrastructure models, strategies and policies should take information warfare models into consideration to aid in mitigating the effects of intentional, accidental and natural disturbances of infrastructures.

Scientia Militaria, South African Journal of Military Studies,
Vol 39, Nr 2, 2011, pp. 52-75.
doi: 10.5787/39-2-114

The article aims to illustrate the relevance of information warfare models to critical infrastructure protection. The scope of the article is broad, so as to include all sectors of critical infrastructure. This results in limitations as not all eventualities can be fully discussed. The models discussed may not be applicable to every possible scenario; however, the intention is to illustrate their relevance in many instances. Background to information warfare, critical infrastructures and the inter-dependencies of the various infrastructure sectors are provided below. The following sections discuss the information warfare models and apply these models to critical infrastructure protection.

Information warfare

As information warfare is still developing, there is no standard definition. The existing definitions reflect the perspective of the particular organisation, nation or individuals. A number of definitions from various sources are provided below:

- “Information warfare is combat operations in a high-tech battlefield environment in which both sides use information-technology means, equipment, or systems in a rivalry over the power to obtain, control, and use information.”[2]
- “Actions taken to affect adversary information and information systems while defending one's own information and information systems.”[3]
- “Offensive and defensive operations against information resources of a "win-lose" nature. It is conducted because information resources have value to people. Offensive operations aim to increase this value for the offence while decreasing it for the defence. Defensive operations seek to counter potential losses in value.”[4]
- Hutchinson and Warren state that the objectives of information warfare is to gain an advantage over a competitor or adversary through the use of one’s own information and related systems, to defend one’s own information and related systems against intentional or accidental harm, and to develop strategies to produce detrimental effects on any adversary or competitor.[5]
- Jones, Kovacich and Luzwick provide the same definition as the Joint Chiefs of Staff; however, Jones, Kovacich and Luzwick provide specific definitions for offensive and defensive information warfare. Offensive information warfare aims to make an adversary “bend to the will of the attacker”, while defensive information warfare "is the ability to protect and defend" the information environment.[6]
- A South African definition is provided by Brazzoli: “All actions taken to defend the military’s information-based processes, information systems and communications networks and to destroy, neutralise or exploit the enemy’s similar capabilities within the physical, information and cognitive domains.”[7]

All of the above definitions make it clear that "information warfare" refers to actions that are taken to protect and attack information and related processes and systems to varying degrees. Brazzoli, however, specifically mentions that these actions may be conducted in three domains: the physical, information and cognitive. The importance of these will be discussed below.[8] Summarising the definitions, a broader definition may be arrived at, namely "information warfare" refers to actions taken to defend, attack or exploit information and related processes and systems in the physical, information and cognitive domain.

Critical infrastructures

Critical infrastructures are those that are vital to the wellbeing and functioning of an organisation, society or nation. Any disturbance of these infrastructures will result in a severe degradation or prevention of operational capabilities and service delivery. A formal definition for critical infrastructures provided in the American Presidential Decision Directive 63 of 1998 is "those physical and cyber-based systems essential to the minimum operation of the economy and government". [9] A more recent definition provided by the US Department of Homeland Security defines critical infrastructure as "the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof".[10] As with the definition of information warfare, the definition of what constitutes a critical infrastructure varies according to organisational or national perspective. In the United States, the President's Commission for Critical Infrastructure Protection (PCCIP) identifies five main critical infrastructure sectors, namely Information and Communications, Banking and Finance, Energy (electrical power, oil and gas), Physical Distribution, and Vital Human Services.[11]

Macaulay provides a similar set of critical infrastructure sectors; however, he divides the vital human services into health services, safety and security, government, and food and water supply.[12] There are interdependencies amongst the sectors. Energy is relied upon in varying degrees by the other sectors, as is information and communications.[13] Large disturbances of these sectors will result in severe disruptions in the financial sector and some vital services, and to a lesser degree in the physical distribution sector. Banking and finance can be considered to be indirectly relied upon by the other sectors, as a disruption will not immediately result in noticeable effects in the information, energy or physical distribution sectors. Figure 1 shows the relationships between the various sectors in more detail.

Infrastructures generally have day-to-day occurrences that degrade performance, or result in interruptions or outages of services. Ware coins the term “infrastructure noise”, borrowing the term from the concept of engineering noise, which interferes with electronic or audio signals. Examples of infrastructure noise may include road accidents, transients or outages on the power grid, communications networks or other services, and daily criminal activity.[14] These incidents are expected in a day-to-day scenario, and measures have been taken to mitigate their effects. This is effectively the noise floor.[15] This concept of noise is relevant to critical infrastructure protection, as a deliberate attack needs to be distinguished from the noise to be able to respond effectively.

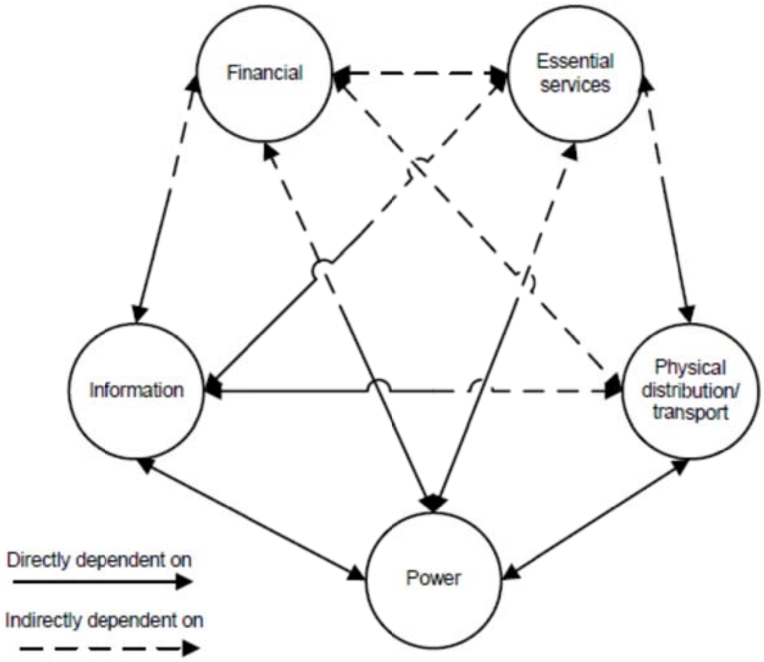

Figure 1: Infrastructure interdependencies

From the interdependencies and noise concept, it is possible to model a number of critical infrastructures as an information or communications network. The distribution of electrical power is via a voltage waveform, and is subject to spikes or dips in the voltage (noise) similar to an analogue communications signal. The power signals may undergo conversions at substations prior to further distribution to the end-users. Similarly, the physical distribution infrastructure may be modelled on a digital communications system, where the vehicles are analogous to bits or packets, intersections for routers or switches, and bridges for gateways. As humans are capable of gathering, storing and processing information (through their senses, memory and thought processes), and humans travel largely along the physical distribution infrastructure, the physical distribution infrastructure can be seen as a system for transporting information.

Information warfare models

This section will discuss the information warfare models and constructs that are relevant to critical infrastructure protection. In some instances, various models will be compared, and a fundamental model will be developed.

Information warfare domains

The definition of information warfare provided by the South African National Defence Force states that information warfare can be conducted in the "physical, information and cognitive domains".[16] Waltz provides an extension to this, where the cognitive domain is further divided into perception and will.[17] Various information systems models also break information systems down into analogous categories. Table 1 compares various models from O'Brien and Marakas,[18] Lehman and Quilling,[19] and Laudon and Laudon.[20] From this, it can be seen that the distinction of physical, information and cognitive domains can be considered the most fundamental model.

Information warfare has significant military connotations; however, it is applicable to other domains as well. Schwartau divides information warfare into personal, corporate and global spheres,[21] whereas Cronin and Crawford discuss it in corporate/economic, community/social, and personal spheres.[22] Schwartau's global information warfare may incorporate international economic competition and information warfare, military information warfare, political competition and warfare, and, to a certain extent, large-scale social information warfare. There may be overlapping amongst the spheres identified by Schwartau[23] and Cronin and Crawford,[24] as an example of multi-national corporations in fierce competition may constitute information warfare at a global and corporate level. These spheres of information warfare may all be conducted in the physical, information and cognitive domains. Phishing attacks or stolen notebook computers may be used to gain personal information, and corporate information warfare could conceivably extend to arson and theft of documents.

Brazzoli (2007)	**Waltz (1998)**	**Lehmann & Quilling (2009)**	**O'Brien & Marakas (2008)**	**Laudon & Laudon (2010)**
Cognitive	Will	People	People	Persware
	Perception			
Information	Information	Processes	Software	Software
		Software	Networks	
		Data	Data stores	
Physical	Physical	Hardware	Hardware	Hardware

Table 1: Comparison of information warfare and information systems models

The Chinese information warfare theories have a greater emphasis on the non-technological aspects, such as social implications or physical means to achieve the same results because their perceived enemy is thought to be technologically superior.[25] This doctrine also advocates the disruption of logistics and communications and pre-emptive strikes, viewing information warfare as a form of unconventional warfare, as opposed to a force multiplier.[26] These possible pre-emptive strikes on communications and logistics may be conducted using computer-based information warfare or physical attacks. Such operations would therefore fall into the information and physical domains.[27]

Information warfare constructs

The South African National Defence Force identifies six pillars of information warfare (also shown in Figure 2) as described by Brazzoli[28] and Théron:[29]

- Command and control warfare, which protects the ability to effectively command and control forces and attempts to hinder an oppositions' command and control capabilities;
- Intelligence-based warfare maximises the intelligence gathering, assessment and dissemination capabilities and degrades those of the opposition;
- Information infrastructure warfare defends friendly information infrastructure and supporting energy infrastructure whilst attacking or exploiting those of the opposition;
- Electronic warfare prevents the opposition's use of the electromagnetic spectrum, while preserving its availability for friendly use;
- Network warfare protects friendly information networks and attacks or exploits the opposition's information networks; and
- Psychological operations, which are activities that are planned and co-ordinated to influence the emotions, reasoning and behaviour of a target audience to further certain objectives.

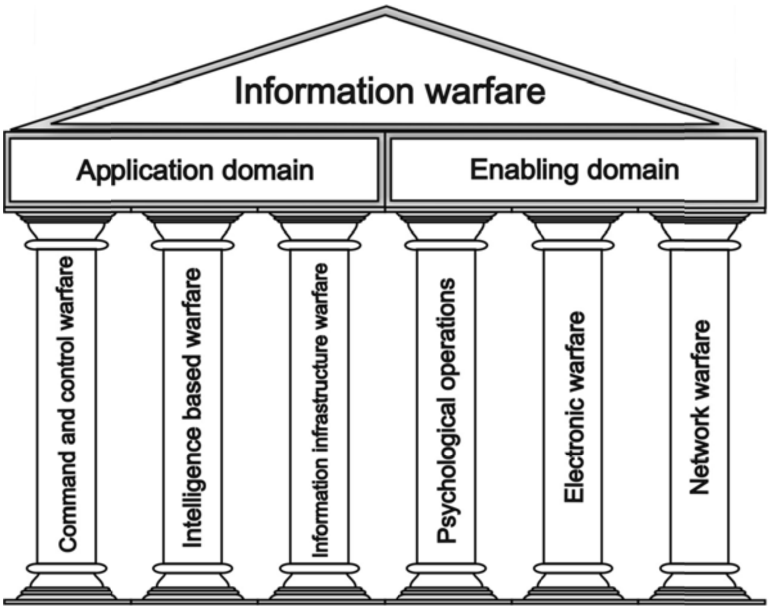

Figure 2: Information warfare functional areas. Source: Brazzoli[30] and Théron[31]

The pillars can then be divided into two groups: the application domain, comprising of command and control warfare, intelligence-based warfare and information infrastructure warfare, and the enabling domain comprising of electronic warfare, network warfare and psychological operations (PSYOP).[32] The pillars in the application domain can be considered to be the targets which are affected, and the enabling domain is where activities are performed to create effects in the application domain. This can be considered to be the weapons which attack or defend the pillars in the application domain, analogous to a sword and shield of old.

The Chinese mention seven pillars: electronic warfare, tactical deception, strategic deterrence, propaganda warfare, psychological warfare, computer warfare, and command and control warfare.[33] The Information Operations Construct of the US Air Force (USAF) illustrates the extension of information warfare to information operations by including information utilisation in warfare and the constituent tactics of information warfare.[34] Figure 3 is an adaptation of the USAF information operations construct, including the concept of information warfare being employed by the corporate sectors and during peace.

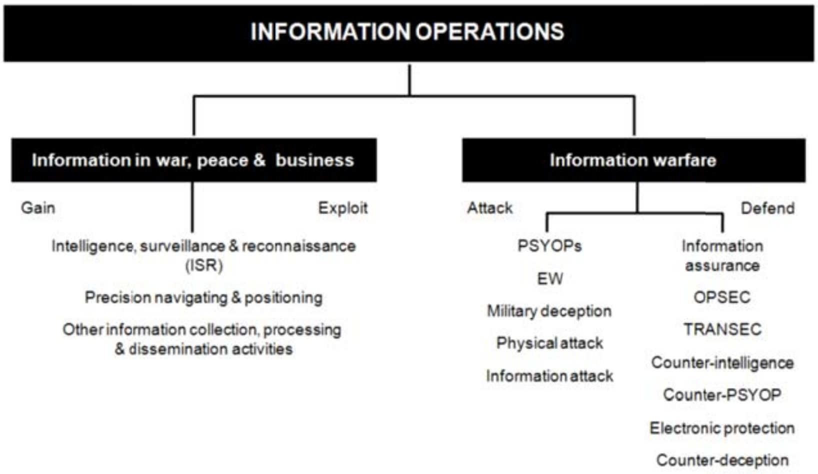

Figure 3: Information Operations Construct. Source: USAF[35]

Attributes of secure information

The CIA model, also known as the CIA Triad, comprise of three aspects of information and the associated infrastructure that needs to be maintained to provide effective security.[36] The three aspects are:

- Confidentiality: access to sensitive information, including knowledge of the functioning and characteristics of infrastructures, which should not be disclosed to unauthorised individuals or systems;[37]
- Integrity: only authorised persons should be able to alter information or systems settings that could affect the infrastructure; and
- Availability: the information and its supporting infrastructure should be available when required and in a form that is understandable.

Waltz extends the CIA Triad to include authentication, non-repudiation and restoration.[38] Authentication ensures that only authorised persons can access relevant restricted information or infrastructure, non-repudiation ensures that a false denial may not call integrity into question, and restoration ensures that information and infrastructure operations may continue should a disturbance occur.[39] These three factors may be considered as subsets of the CIA Triad: authentication seeks to maintain confidentiality and integrity, non-repudiation protects integrity, and restoration aims at preserving availability.

Parker expands on the CIA Triad, proposing possession or control, authenticity and utility as three extra attributes.[40] Possession and control are concerned with the fact that control or possession of the information may be lost, yet the confidentiality has not been breached unless the information has actually been “read”. This may be considered as a unique aspect of confidentiality, as the information has been accessed in some form, then confidentiality has been breached, and possibly availability should the rightful owner also have lost physical control of the information. Authenticity refers to the correct attribution of information to a source or field in a database, and such authenticity is breached should such information be incorrect. This may be considered as a subset of integrity, as an error or incorrect attribution reduces the quality of the information. Utility refers to the usefulness of the information. It is argued that should a decryption key be lost, all aspects of information are preserved; however, it can be counter-argued that the information is not actually available and cannot be used as intended as it cannot be accessed, hence utility is a subset of availability and integrity.

From the discussions above considering Waltz and Parker, it can be seen that the CIA Triad constitutes the fundamental attributes of information and associated infrastructures. The extensions proposed may be considered as subsets of the three constituents of the CIA Triad.

Information warfare attack

The Borden-Kopp model was developed independently by Borden[41] and Kopp,[42] and is one of the primary mathematical models of information warfare. The Borden-Kopp model is based on Shannon's information theorem, which determines the amount of information (in bits) that can be successfully transmitted through a noisy communications channel.[43] By introducing “noise” in various manners one can degrade, corrupt, or deny the information supply to an adversary, and by intercepting the signal one can exploit the information. Degrading of information refers to delaying the arrival of such information, or destroying it in full or part, so that it has reduced value. An example is jamming of wireless communications, thereby reducing the capacity of the channel and delaying or preventing the data transmission.[44] Denial implies preventing access or use by direct attack, such as physical destruction or blinding of a sensor. Information may be corrupted by inserting false information, in other words contaminating the data. Exploitation refers to the act of intercepting an adversary's information, or increasing the availability of friendly information to improve efficiency.[45]

Waltz (1998)	**Borden-Kopp**	**Hutchinson & Warren (2001)**	**Pfleeger & Pfleeger (2003)**	**USAF (1998)**
Disrupt	Degrade Deny	Disrupt Deny Destroy	Interrupt	Deny Destroy
Corrupt	Corrupt	Manipulate Alter perception Change context	Modify Fabricate	Deceive/corrupt
Exploit	Exploit	Steal	Intercept	Compromise

Table 2: Comparison of information warfare attack models

Hutchinson and Warren follow a similar model, where the actions that may be taken against data are denial, disruption and destruction, stealing and manipulation, and actions taken against the cognitive domain are changing the context or perceptions with which the data or information is viewed.[46] This is virtually identical to the Borden-Kopp model, except for the change in terms and the fact that "corrupt" has been split into manipulation, altered perception and changed context. Pfleeger and Pfleeger again illustrate a similar model, comprising of interception (exploitation), interruption (denial and degradation), modification and fabrication, where the latter two may be considered as forms of corruption.[47] Waltz provides a simpler model consisting of disruption, corruption and exploitation, which directly attack availability, integrity and confidentiality.[48] Table 2 compares the four models discussed above and that of the USAF.[49] The model proposed by Waltz can be seen as the fundamental model, while the other sources distinguish between specific elements contained in the "disrupt" and "corrupt" categories.

Table 3 lists information warfare threats that can be used to implement the attack types. Many threat types, such as malicious code and system intrusion, may be used to meet different objectives. Malicious code and software bugs often aid in system intrusions, which are often done in an attempt to access confidential information.

Compromise	**Deception/corruption**	**Denial/loss**	**Destruction**
Malicious code System intrusion Psychological operations Intelligence collection Technology transfer Software bugs	Malicious code System intrusion Military deception Spoofing Imitation	Malicious code System intrusion Lasers Physical attack Electro-magnetic pulse Virus insertion System overload Radio frequency jamming	Malicious code Bombs Directed energy weapons Lasers Physical attack Electro-magnetic pulse Biological & chemical warfare

Table 3: Information warfare threats, adapted from USAF[50]

Table 4 lists the tools and tactics of the three functional areas in the enabling domain for the various information warfare attack methodologies. Denial-of-service attacks are of concern as many critical infrastructures rely on computer networks. This type of attack prevents legitimate network traffic, thereby negatively impacting on any computer-based communication. Similarly, radio frequency jamming, intentional or accidental, will hinder any communications using the wireless channel, and negatively impact on the systems that rely on that channel.

	Electronic warfare	**Network warfare**	**PSYOPs**
Disrupt/deny/ destroy	Radio frequency jamming Anti-radiation missile Low observability technology	Denial-of-service attack Physical destruction Delete information Firewalls	Disrupt and deny communications and media broadcasts via electronic warfare, network warfare and physical destruction
Exploit	Signals intelligence Communications intelligence Electronic intelligence Identification friend or foe	Sniffers Scanners System intrusion Backdoors Intrusion detection systems	Release and distribute condemning information Counter-propaganda Perception management
Corrupt	Chaff Flares Low observability technology	Honey pots Honey nets Root-kits Malware	Provide information out of context Counter-propaganda Propaganda Perception management

Table 4: Information warfare tactics and tools for the enabling domain, adapted from Van Niekerk[51] and Smith and Knight.[52]

Information warfare targets

Elements of an information system or infrastructure that are subject to being targeted in an attack are:[53]

- stores or containers, such as disk drives and computer and human memories, which can have their contents corrupted or which can be physically damaged or destroyed;
- transporters, such as humans and telecommunication systems, which may have their performance degraded by a denial of service attack, or which may be intercepted to exploit the information;
- sensors, such as cameras and human input devices, which could be destroyed or fed false signals;
- writers or recorders, such as printers and disk writers, which can have the output stream of data corrupted; and
- processors, which include software in addition to microprocessors and humans and which may be corrupted by altering the logic, or be subjected to degradation or destruction.

Summary

The information warfare models that have been discussed describe the domains in which information warfare exists, the constituents of information warfare, concepts for attacking and defending, and potential targets. This section sought to compare models of information warfare and extract a fundamental model. From the models discussed above, it is clear that information warfare can be applied to the physical, information and cognitive domains. Secure information has three primary attributes: confidentiality, integrity and availability. These attributes are attack through exploitation, corruption and disruption (denial, degradation and destruction). Attacks may target the stores, transporters, sensors, recorders and processors of the infrastructure. The following section aims to show the relevance of these models to all critical infrastructure sectors.

Application of information warfare models to critical infrastructure protection

This section shows how the information warfare models discussed above can be applied to critical infrastructures to illustrate the relevance of these infrastructures at a fundamental level, and possible implications for the military. The information warfare models may not be relevant all scenarios; the intent is to show a broader applicability of the models.

Information warfare domains

Information and communications infrastructures can be divided into the physical, information and cognitive domains, as described in the previous section. This section illustrates the applicability of this domain model to all critical infrastructure sectors. The physical distribution infrastructure consists of a physical component in the form of roads, ports and so forth. The information component consists of traffic rules and signs (for air, sea and land transportation), and the cognitive component incorporates the people using and controlling the infrastructures and traffic, who are making decisions related to information and their knowledge. The physical domain of the energy sector comprises of the power stations, fuel stores, power lines and pipelines. The information domain comprises of the controls, procedures and the electrical signals themselves, and the cognitive domain consists of the people as it does in the case of the information and physical distribution sectors. Likewise, the essential services and financial sectors can be divided into physical, information and cognitive domains. These sectors have decision-makers which fall into the cognitive domain, procedures and data, such as financial indicators, that reside in the information domain, and physical hardware, such as water pipes and teller machines.

The Chinese concept of using pre-emptive strikes to disrupt communication and logistics would ideally target critical distribution and information infrastructures through computer-based information attacks or physical attacks.[54] Computer attacks could crash logistics management systems, air-traffic control systems or other communications systems. Physical attacks could destroy key bridges or equipment at ports. Such attacks could be used to delay the arrival of military forces to the conflict zone or possibly form part of an economic information war should the computer attacks target financial systems, whereas the physical distribution of goods is hindered by physical attacks.[55] The nature of the Chinese doctrine is asymmetric, almost guerrilla warfare-like in style, while information warfare can be used to erode a superior adversary’s ability to conduct military operations by attacking critical infrastructures and disrupting the command and control, intelligence and logistics of the adversary.[56] These tactics could conceivably be employed by non-state actors against a nation state, if the nation state is considered as a superior enemy of the non-state actors. Such attacks, where abilities in the physical and information domains are eroded, will impact on the cognitive domain, as the necessary tools and information for decision-making may not be available or accurate.

Information warfare constructs

In this section, the relevance of the information warfare functional areas to critical infrastructure protection is discussed; however, all constituents of information warfare may not be applicable to all sectors. As described above, information warfare consists of six main functional areas: intelligence-based warfare, network warfare, electronic warfare, PSYOPs, command and control warfare, and information infrastructure warfare.

As described previously, information infrastructure warfare includes the supporting energy infrastructure, and it was shown that physical distribution might be considered to be a means of communication and information transport; therefore, information infrastructure warfare may be considered to include actions taken to attack or defend the information and communication, physical distribution and energy sectors. Intelligence-based warfare is relevant in terms of assessing threats and risk to infrastructure. Preventing an aggressor from acquiring adequate intelligence regarding the infrastructure to successfully mount an attack would also be classified under this category. Information security, operational security and deception may be used as defensive tools in intelligence-based warfare and in protecting infrastructures.

As electronic warfare targets the electro-magnetic spectrum, only sections of infrastructures employing radio communication systems will be targeted. Similarly, network warfare targets computer networks; again, only infrastructures reliant on networks will be impacted upon. Naturally, the information and communications sector is the primary target; however, infrastructures reliant on this sector may also be vulnerable, for example air traffic control uses radar, resulting in a vulnerability of the physical distribution infrastructure to electronic warfare.

PSYOP techniques may be used for deterrence from attacks by convincing potential attackers that it is not worth the effort, as the retaliation or consequences of an attack will be severe and may dissuade many from making an attempt. This may be done at a local level, such as within a community or state, or across national boundaries, what the Chinese call “strategic deterrence”. Strict security policies may also act as deterrence.

Electronic protection applies primarily to the information and energy sectors, where protection is given against intentional, accidental and environmental occurrences that may disrupt the infrastructure. This may include lightning protection, shielding against electro-magnetic interference and the effects of solar storms, and surge protectors and uninterruptible power supplies to protect from transients in the electrical distribution. These techniques may be used to protect information systems that support critical sectors, such as hospital equipment, process controllers for waterworks and emergency services systems.

Secure information attributes model

As in the case of information, infrastructure is only useful if it is available when required. Physical distribution, such as roads and airports, power distribution and generation facilities, and emergency services hotlines will serve no purpose if they exist but are completely unavailable for any reason. The concept of availability from information security therefore holds true for all infrastructures.

The concept of integrity regarding infrastructure is similar to the concept of availability. An infrastructure's integrity is compromised should it be unable to operate at full capacity or should some of the functions be unavailable. An example would be an airport which is unable to use all of its runways due to damage, or where operations are restricted to light aircraft when full capabilities would include large commercial aircraft. Another example could be emergency services' response time being degraded due to the unavailability of a number of vehicles or personnel.

Keeping certain details of infrastructure operations or physical characteristics confidential may aid in protection. An attacker that is denied information regarding the critical components of an infrastructure may be forced to attack arbitrarily, or such attacker may spread smaller attacks over more targets in the hope of disabling the intended target. This may result in the integrity of a number of non-essential components being degraded, as opposed to the critical elements becoming unavailable. For example, an innocuous switching station may contain a vital international link. Without this knowledge, attackers may target larger, more impressive-looking switching stations in the hope of severing that link.

Information warfare attack models

The fundamental information warfare attack model as discussed previously constitutes exploitation (affecting confidentiality), corruption (affecting integrity), and disruption (through denial, degradation or destruction, which impacts on availability).

The concept of infrastructure noise, where everyday incidents result in less than optimal performance of an infrastructure, has strong parallels to Shannon's information theorem,[57] on which Borden and Kopp base their information warfare models. In both cases, as the amount of noise increases, there will be a decrease in the performance. The high-level tactics of degradation, denial and corruption hold true for most infrastructures. These are described above in relation to communications and information infrastructure. The electrical power infrastructure may be physically destroyed or damaged, resulting in the denial or degradation of performance. The power distribution may be interfered with in such a way that the electrical signal is corrupted. It will consequently have irregular power values that may further damage portions of the infrastructure or equipment relying on it. Likewise, fuel distribution may be denied or degraded, and as a result may introduce contaminants into the fuel itself, which will result in the supply being corrupted.

The essential services and finance sectors may be denied or degraded by denying or degrading the infrastructures that they depend upon, most notably the information and energy infrastructures. By exploiting the information infrastructure, it may be possible to corrupt the information supporting the essential services, resulting in funds being transferred incorrectly, or inadequate or incorrect responders being dispatched to emergencies. The water supply may also be corrupted by contamination of the supply. The physical distribution sector may be degraded or denied by creating blockages or physically damaging it. Corruption may be achieved by altering navigation signs on roads to create confusion. This was implemented with some success in 1944 by German forces during their offensive in the Ardennes.[58]

Attacking portions of an infrastructure will have a ripple effect. If a bridge were to be destroyed, the noise created would deny its use according to the model, and the road would be degraded in that it cannot perform all of its functions. Other roads and bridges would then also experience an increase in noise and have their performance degraded, causing an increase in traffic finding a new route. This may result in a higher rate of accidents, thereby increasing the noise further. Figure 4 illustrates the case of a computer network and physical distribution across a bridge. For each case, there are three possible routes to carry traffic.

The destruction or denial of a key component in one of the routes increases traffic in the two remaining routes. Similarly, a denial-of-service attack on a specific network or website will also create additional effects. Networks hosting any zombie computers i.e. computers that are under the control of a third party without the knowledge of the legitimate user, that are participating in the attack will also be subject to degraded performance due to the increase in the noise level. Any major international gateways through which the attack traffic travels will also suffer.

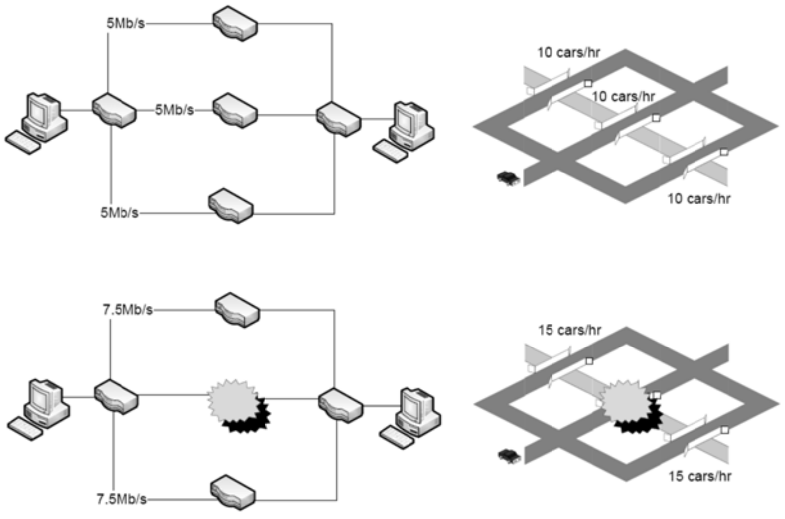

Figure 4: Effects on link traffic due to denial

Targets

As described previously, information warfare targets in the information infrastructure are stores, transporters, sensors, writers or recorders and processors. The relevance of this model to the other four sectors of critical infrastructure is discussed.

The physical distribution sector provides its own transportation, just as computer networks provide the transportation of information; therefore the roads, airports, harbours and the vehicles themselves are the transports. The stores comprise of vehicle pools, hangers and stockpiles of raw materials that are used for production and maintenance of the vehicles and physical infrastructure. The production lines for vehicles and the painters of road or runway signs and markings are analogous to the writers, whereas the radar, traffic cameras and similar technologies are the sensors. The processors are the flight controllers, navigation systems and onboard computers in cars and traffic lights. The transporters in the energy sector are the power lines and pipelines that distribute the electricity and fuel respectively, and the stores are the fuel, coal and gas depots, and hydro-electric or pumped storage dams. The sensors form part of the monitoring control system, such as temperature or flow meters, which provide the computer-based processors with information to control the flow of fuel or the generation of electricity.

The financial and vital human service sectors primarily rely on the physical distribution and information infrastructures for transport; however, water and liquid waste will be transported via pipes. Stores may include dams and reservoirs, medical dispensaries and equipment or armament stores for human services, whereas the treasury and banks will provide storage for physical money, while the virtual money information will be stored in computer-based systems. The production of medicines and the mint are analogous to the writers, but others may be found in the form of card writers and transaction printers in auto-tellers. The sensors may include card readers, flow meters or heart rate monitors amongst others, which again provide inputs to a variety of processors. In all infrastructures, the human carries all types of targets: the senses are the sensors, speech is the recorder, the body is the transporter, and the brain is the processor and storage space. However, the human has other characteristics, such as emotions, thought and perception, which provide cognitive targets, which directly affect the human, which may then have repercussions on various infrastructures due to human error.

From these descriptions, it is clear that all sectors of critical infrastructure contain potential targets for an information warfare attack, which may be conducted either physically or via the information networks to disrupt the controls and management of the respective systems.

The effect of critical infrastructure interdependencies

Due to the interdependencies of critical infrastructures, an attack on a specific infrastructure may have impacts on others. Most notably, attacks on a number of infrastructures may be conducted through the information and communications sector by attacking their controlling information systems. This in particular is what raises the concern of information warfare cyber attacks at a strategic level.[59] As a result of an attack, multiple infrastructures may be impacted. Mass disruption of transport routes and communications would degrade the ability of emergency services to respond, or it may affect the financial and energy sectors in terms of fuel not being transported to the points of sale. In 2009, a banking scam was conducted in South Africa where the organised crime gang diverted short messages containing the passwords sent from online banking websites, enabling them to access the victims' accounts.[60] This illustrates how compromising the cellular telecommunications infrastructure can impact on the financial infrastructure.

As mentioned, the concern is primarily over cyber attacks, where an attack will be targeting the information and communications infrastructure, or be conducted through such infrastructure to attack a process controller or financial system, or just to gather information. A denial-of-service attack on a specific network may increase traffic to such a level that all network-based communications are hindered; thus, emergency services, government agencies and financial institutions will have some or all of their communication hindered. Business and financial services may also be affected, resulting in an economic impact, such as occurred in the cyber attacks on Estonia and Georgia.[61] The penetration of NASDAQ computer systems has raised concerns over the vulnerability of the financial infrastructure to cyber-based attacks.[62] The French Ministry of Finance also experienced penetration of their computer systems.[63] Such attacks breach the confidentiality of both government and economic information. The Stuxnet worm of 2010 again illustrated the vulnerability of the manufacturing and energy sectors, when an Iran nuclear power plant sustained damage as a result of the controlling computer systems being infected by the worm.[64]

Summary

The relevance of information warfare models to critical infrastructure was illustrated. Infrastructures share many attributes with the models, in that the availability and integrity of infrastructures and their components can be degraded and corrupted, and sensitive information regarding the functioning of infrastructures could conceivably be exploited. Infrastructures contain components that can be classified as stores, transporters, recorders, sensors and processors. Not all of these categories will be applicable in every case; however, the classification provides a general guideline for classifying infrastructure components.

The application of the information warfare models is intended to be high-level and to guide classification and thought processes regarding critical infrastructure protection. Information warfare and critical infrastructure are not synonymous, therefore it cannot be expected that the information warfare models will be applicable to all possible scenarios. The relevance is primarily at a broad conceptual level. At this level, it may also be possible to apply the models to environmental incidents; for example, a flood may damage a bridge, thereby reducing the availability and integrity of that bridge. The information warfare attack describes the effect of an incident, in this case disruption, and the secure information attributes describe the impact type, in this case integrity and availability. As the information warfare models are designed for information infrastructures, the application will only hold perfectly for those infrastructures that are information-based (including the financial sector). Information can be intangible, fluid and sometimes "invisible", where breaches may not be noticed for extended periods of time. Where the infrastructure is more physical in nature, such as the distribution sector, which is more rigid and tangible, the application of the models will largely be limited to the physical domain, and only be applicable to the information and cognitive domains where there is direct human involvement.

Conclusion

Information warfare models have a number of variations; however, there are fundamental aspects that apply to most of the variations. These models describe the domains within which information warfare exists and where the constituents, attack and defence methods, and targets of information warfare were ascertained. The study on which this article is based, conceptually investigated the relevance of these fundamental models of information warfare to critical infrastructure protection. Most information warfare concepts may be used to attack all critical infrastructure sectors by various methods, and they do not necessarily rely on the conventionally thought-of cyber attacks. Likewise, the concepts of information security may also be applied to all critical infrastructure sectors in order to protect them, namely to assure the availability and integrity of the infrastructure. It may also be possible for an information warfare attack to create effects in one infrastructure through another. The primary concern in this regard is the reliance of society on information networks, and the possible effects of a cyber-based attack.

Endnotes

[1] Kopp, C. "A fundamental paradigm of infowar". *Systems*, 2000, 47. <http://www.ausairpower.net/OSR-0200.html > Accessed on 25 October 2011.

[2] Baocun, W & Fei, L. "Information warfare". In Pillsbury, M (ed), *Chinese views of future warfare*, Washington, DC: National Defense University Press, 1997, 328. <http://www.au.af.mil/au/awc/awcgate/ndu/chinview/chinapt4.html#8> Accessed on 9 January 2011.

[3] Joint Chiefs of Staff (JCS). *Joint publication 3–13: Joint doctrine for information operations*. Washington, DC: US Department of Defense, 1998, I–1.

[4] Denning, DE. *Information warfare and security*. Boston, MA: Addison-Wesley, 1999, 21.

[5] Hutchinson, W & Warren, M. *Information warfare: Corporate attack and defense in a digital world*. Oxford: Butterworth Heinemann, 2001, xx.

[6] Jones, A, Kovacich, GL & Luzwick, PG. *Global information warfare*. Boca Raton: Auerbach, 2002, 24.

[7] Brazzoli, MS. "Future prospects of information warfare and particularly psychological operations". In Le Roux, L (ed), *South African Army vision 2020*, Pretoria: Institute for Security Studies, 2007, 219.

[8] *Ibid.*, pp. 219–220.

[9] Moteff, J & Parfomack, P. *Critical infrastructure and key assets: Definition and identification*. Washington, DC: Congressional Research Service, 2004, 4.

[10] Department of Homeland Security. "Critical infrastructure and key resources". 5 April 2010. <http://www.dhs.gov/files/programs/gc_1189168948944.shtm> Accessed on 25 May 2010.

[11] Ware, WH. *The cyber posture of the national information infrastructure*. Santa Monica, CA: RAND Institute, 1998, 4.

[12] Macaulay, T. *Critical infrastructure*. Boca Raton: CRC Press, 2009, 10.

[13] *Ibid.*, pp. 12–16.

[14] Ware *op. cit.*, pp. 10–11.

[15] *Ibid.*, p. 11.

[16] Brazzoli *op. cit.*, p. 219.

[17] Waltz, E. *Information warfare: Principles and operations*. Boston, MA: Artech House, 1998, 4–5.

[18] O'Brien, JA & Marakas, G. *Introduction to information systems*, 14th edition. New York: McGraw-Hill, 2008, 30.

[19] Lehmann, H & Quilling, R. "Why are there not more grounded theories of information systems?" Paper presented at the Business and Management Conference, Durban, 5–7 November 2009.

[20] Laudon, KC & Laudon, JP. *Management information systems: Managing the digital firm*, 11th edition. Upper Saddle River, NJ: Prentice Hall, 2010, 42.

[21] Schwartau, W. *Information warfare: Chaos on the information superhighway*, 2nd edition. New York: Thunder's Mouth Press, 1996, 18–19.

[22] Cronin, B & Crawford, H. "Information warfare: Its application in military and civilian contexts". *The Information Society* 15/4. 1999. 259–261.

[23] Schwartau *op. cit.*, pp. 18–19.

[24] Cronin & Crawford *op. cit.*, pp. 259–262.

[25] Mulvenon, JC. "The PLA and information warfare". *Proceedings of The People's Liberation Army in the Information Age*. San Diego: RAND Corporation, 1998, 184; Rawnsley, GD. "Old wine in new bottles: China-Taiwan computer-based 'information warfare' and propaganda". *International Affairs* 81/5. 2005. 1069; PuFeng, W. "The challenge of information warfare". In Pillsbury *op. cit.*, p. 319.

[26] Mulvenon *op. cit.*, p. 183.

[27] Rawnsley *op. cit.*, p. 1070.

[28] Brazzoli *op. cit.*, p. 221.

[29] Théron, J. "Operational battle space: An information warfare perspective". In Phahlamohlaka, J, Veerasamy, N, Leenan, L & Modise, M (eds), *IFIP TC9 Proceedings on ICT uses in Warfare and the Safeguarding of Peace*, Pretoria: CSIR, 2008, 42.

[30] Brazzoli *op. cit.*, p. 221.

[31] Théron *op. cit.*, p. 42.

[32] *Ibid.*; Brazzoli *op. cit.*, p. 222.

[33] Mulvenon *op. cit.*, p. 182.

[34] United States Air Force (USAF). *Air Force Doctrine Document 2–5: Information Operations*. Washington, DC: US Department of Defense, 1998, 3.

[35] *Ibid*.

[36] Denning *op. cit.*, p. 41; Waltz *op. cit.*, p. 22.

[37] Whitman, ME & Mattord, HJ. *Management of information security*, 3rd edition. Boston, MA: Cengage Course Technology, 2010, 513.

[38] Waltz *op. cit.*, pp. 301–302.

[39] *Ibid.*, p. 302.

[40] Parker, DB. "Toward a new framework for information security". In Bosworth, S & Kabay, ME (eds), *Computer security handbook*, 4th edition, New York: Wiley, 2002, 5·9.

[41] Borden, A. "What is information warfare?" *Aerospace Power Chronicles*, Contributer's Corner 1999. <http://www.airpower.maxwell.af.mil/airchronicles/cc/borden.html> Accessed on 2 July 2009.

[42] Kopp *op. cit.*, pp. 47–55.

[43] Shannon, CE. "A mathematical theory of communications". *Bell Systems Technical Journal* 3/27. 1948. 379–423.

[44] Kopp *op. cit.*, pp. 47–55; Borden *op. cit.*

[45] *Ibid.*; Kopp *op. cit.*, pp. 47–55.

[46] Hutchinson & Warren *op. cit.*, p. 3.

[47] Pfeeger, P & Pfleeger, S. *Security in computing*, 3rd edition. Upper Saddle River, NJ: Prentice Hall, 2003, 36.

[48] Waltz *op. cit.*, p. 23.

[49] United States Air Force (USAF) *op. cit.*, p. 6.

[50] *Ibid*.

[51] Van Niekerk, B. "Interoperability in CNO and EW: Considerations for the African continent". Paper presented at the Military Information and Communications Symposium of South Africa, Pretoria, 20–24 July 2009.

[52] Smith, R & Knight, S. "Applying electronic warfare solutions to network security". *Canadian Military Journal* 6/3. 2005. 53. <http://www.journal.forces.gc.ca/vo6/no3/electron-eng.asp> Accessed on 25 May 2010.

[53] Hutchinson & Warren *op. cit.*, p. 9.

[54] Mulvenon, *op. cit.*, p. 183.

[55] *Ibid.*, p. 185.

[56] Ventre, D. *Information warfare*. London: ISTE, 2009, 88.
[57] Shannon *op. cit.*, pp. 379–423.
[58] Lucas, J. *Kommando: German Special Forces of World War Two.* London: Cassell, 1998.
[59] Ware *op. cit.*, p. 2; Molander, RC, Wilson, PA, Mussington, DA & Mesic, RF. *Strategic information warfare rising*. Santa Monica, CA: RAND Institute, 1998, 3–4; Anderson, RH, Feldman, PM, Gerwehr, S et al. *Securing the US defense information infrastructure: A proposed approach*. Santa Monica, CA: RAND Institute, 1999, 6.
[60] Van Rooyen, K. “Hidden price of a banking scam”. *The Sunday Times.* 19 July 2009, 9.
[61] Hart, K. “Longtime battle lines are recast in Russia and Georgia’s cyberwar”. *The Washington Post.* 14 August 2008, D01; Rolski, T. “Estonia: Ground zero for world’s first cyber war?” *ABC News.* 17 May 2007. <http://abcnews.go.com/print?id=3184122> Accessed on 23 September 2009.
[62] Donohue, B. “NASDAQ hack raises critical infrastructure concerns”. Threatpost Blog. 7 February 2011. <http://threatpost.com/en_us/blogs/nasdaq-hacked-unknown-hackers-unknown-reasons-020711> Accessed on 9 February 2011.
[63] Roberts, P. “Report: French Ministry of Finance confirms hack”. Threatpost Blog. 7 March 2011. <http://threatpost.com/en_us/blogs/report-french-ministry-finance-confirms-hack-030711> Accessed on 8 March 2011.
[64] StrategyPage.com. “Stuxnet takes it up a level”. 3 October 2010. <http://www.strategypage.com/htmw/htiw/articles/20101003.aspx> Accessed on 4 October 2010.