INFORMATION WARFARE: CHANGING TRADITIONAL NOTIONS OF AGGRESSION

Tanya Ross-Gadsden discusses the need for regulators to recognise the impact individuals have in cyberspace, and how individualised "cyberweapons" reshape traditional notions of aggression.

With the advent and proliferation of the Internet, information has become accessible to computer users of all descriptions. It is simple to interface with usergroups, exchange information and knowledge, or create individual Internet sites. This environment also reshapes the concepts of force, aggression, and warfare as the tools of war no longer belong to nation states. Technology has accelerated social interaction exponentially, yet municipal regulation and public international law have failed to keep pace. To some, cyberspace represents a new frontier akin to the wild American west of the early 1800's. In this environment, rule making will require a combination of law, regulation, education and training of users, as well as the cooperation of countries worldwide.

What authors do not mention is the way in which laws of the physical world must change in order to effectively operate within this new frontier. In this way, Information Warfare, as an exercise in information and systems control, threatens governments, groups and individuals.

This paper seeks to outline the challenges cyberspace and Information Warfare ("IW") pose to the traditional notion of force. First, the law of force, and its use by states, will be briefly outlined. Second, the pervasive and transnational nature of the electronic battlefield will be illustrated through definitions of IW. Finally, the public/private divide will be explored in an effort to test its strength and value on the electronic battlefield.

TRADITIONAL NOTIONS REVISITED

Since the *Treaty of Westphalia* in 1648, international law has been comprised of sovereign state actors who contract with one another through treaties of consensus. Sovereignty implies that a nation is not subject to the will of another, and that it is an independent actor in international relations.

Sovereign actors are prohibited from using force by the United Nations charter Article 2(4) qualified only by the right to self defence. In support of this prohibition, states' adversarial interaction is based on at least four assumptions. First, public international law is the law governing relations between states. Second, war, as regulated by public international law, is an adversarial exercise between states. Third, an actor engaging in war requires a strong national economy, industrial manufacturing capacity and a population from which to recruit a military force. Lastly, implicit in the first and third assumptions, non-state actors, groups, and individuals are not subject to public international law and are therefore not bound by its traditional notions.

In contrast, cyberspace is an electronic construct created by the interconnectivity of global communications systems and as such it has the power to overturn these fundamental assumptions. Through its multi-jurisdictional personality cyber-space facilitates the deconstruction of our highly structured and standardised society. Cyberspace can be differentiated from the international environment which constructed public international law because it lacks both boundaries and a physical presence and, as a result, cyber-citizens may maintain a sense of anonymity; reincarnating endlessly free of the confines of linear time. It is no longer necessary to measure aggression and military capability in arms and munitions. Cyberspace is responsible for introducing the individual to the

weaponry of information warfare through the personal computer.

WHAT IS INFORMATION WARFARE?

In order to understand the individualised nature of cyber-weaponry, it is necessary to understand what is meant by the term IW. Attempting to identify a comprehensive definition of IW, however, is not an easy task. Such a search may be in vain because of the ever changing nature and developing possibilities electronic interconnectivity present to society. In spite of this warning individuals, institutions and different branches of the United States military have created definitions of IW that reflect their own needs and perceptions. For example the Institute for the Advanced Study of Information Warfare ("IASIW") states that:

> *"Information warfare is the offensive and defensive use of information and information systems to exploit, corrupt, or destroy an adversary's information and information systems, while protecting one's own. Such actions are designed to achieve advantages over military or business adversaries."*[1]

The advantage of the IASIW's definition is that it incorporates non-military interests as the subject of IW. It is the references to military or business adversaries that provide context for the words "offensive", "defensive" and "military", indicating that there might be an organisation behind IW activity. This is important since an organisational hierarchy would be able to provide operations, resources, and complex electronic systems through which to camouflage IW activities.

Alternatively, in more sweeping terms, IW has been said to be:

> *"The strategic, operation, and tactical level competitions across the spectrum of peace, crisis, crisis escalation, conflict, war, war termination, and reconstitution/ restoration, waged between competitors, adversaries or enemies using information means to achieve their objectives."*

This definition may be far too broad, and may also apply generally to social and political activity[2]. It also incorporates levels of organisation which could be labelled "strategic" or "tactical" which may not always be suitable when attempting to identify an information warrior. Perhaps a more fitting and inclusive notion of IW is the definition of Colonel Richard Szafranski USAF instructor at the American Airforce Air War College. Szafranski's definition illustrates the potential IW holds for individuals. He says:

> *"Information warfare is a form of conflict that attacks information systems directly as a means to attack adversary knowledge or beliefs. Information warfare can be prosecuted as a component of a larger and more comprehensive set of hostile activities –a netwar or cyberwar – or it can be undertaken as the sole form of hostile activity."*[3]

The Colonel has identified IW simply as a form of conflict which may or may not be an element of a larger tactical operation. He also demonstrates that IW is an umbrella term, incorporating *netwar* or *cyberwar* activities which may operate independently. Essentially, this definition does not explicitly apply to, nor does it exclude, an individual or group not aligned to any legitimate government or government agency. Evidence of this is the Colonel's examples of *netwar* and *cyberwar*. Although each involves a different use of technology and each aims to produce different outcomes, they are both defined in national or political terms.

Netwar has been defined as "information related conflict, at a grand level, between nations or societies"[4]. It involves disrupting what the target population knows or believes to know about the world. This includes psychological campaigns and propaganda, subversion and infiltration of electronic networks and databases, and efforts to promote dissident or opposition movements[5].

Cyberwar is less pervasive and focuses on supplementing military operations with information related to, and intended to facilitate, those operations[6]. The Gulf War, in much the same way as the current military operations in Kosovo, was an example of *Cyberwar*. Operations in the Gulf, including the destruction of Iraq's information systems and the application of information to reduce Allied consumption of capital and labour, were employed to immobilise Iraq's military leaders. Perhaps the greatest weakness of Szafranski's definition is its reliance on conflict. Conflict requires more than one party knowingly engaging in a struggle of opposing interests. In contrast, the demassification of society's information systems, brought about by cyberspace, negates the need for opposing parties.

Essentially, all of these definitions ignore the use of IW by individuals and groups as well as cyber-terrorists and cyber-extortionists. Even IW in the guise of *netwar* or *cyberwar* excludes the home office warrior. Clearly a new definition of IW is required that acknowledges the availability of IW weaponry to, and its use by, those individuals and groups not traditionally subject to international law.

BROADENING THE BATTLEFIELD

Cyber-terrorism is a creature of cyberspace and terrorists are currently active in extorting financial institutions. The cyber-terrorists use advanced techniques, often learned from the military, to threaten the integrity of banks and broking firms and demonstrate their ability to cause "computer meltdowns" to extort vast sums of money from the target institution. The funds demanded are transferred electronically into a remote account nominated by the terrorists only to be 'zapped' out moments later.

The weapons of IW have been described as "modern plagues" and include:

> *"The Logic Bomb"*: A coded device that may be detonated remotely. Once activated the "bomb" eats data and has the potential to destroy any electronic system including those systems that control rail, air, and road traffic.
>
> *"High emission radio frequency guns"*: This weapon "blows" an "electronic wind" through the target computer system.
>
> *"Viruses"*: the lowly virus has evolved to become ever more complex. They exist in many forms and may lay dormant depending upon their programme. A virus can be constructed with the capability to destroy an entire telephone communications system. Some virus bombs may be attached to an e-mail and, once inside the target system, begin writing over all disc application, data and communications files such as the recent Explore.zip and Melissa viruses.

Individuals are able to use this electronic arsenal against governments, governmental organisations, business, industry and other individuals. Hence, the meta-jurisdictional nature of

cyberspace and the nature of cyber-weaponry merge physical theatres of war into one unique battlespace.

MERGING PUBLIC AND PRIVATE

Government and private agencies have considered the problems an electronic attack could present to an advanced information society. A hypothetical scenario included intermittent interruptions to the power grid, telephone line crashes, collisions of misinformed transporter trains, and "softwar" (the use of television broadcasting systems to publicise propaganda). Leaders in IW research were given fifty minutes to find a solution to the hypothetical havoc caused by the unidentified information warriors[7]. The value of this exercise is illustrated in the four main conclusions reached by the participants:

1. IW is inexpensive;
2. Cyberspace knows no geographic or theoretical boundaries such as national borders or the public / private divide;
3. Perception is easily manipulated in cyberspace and widely disseminated;
4. Cyberspace represents a battlefield with no discernible front line. Therefore analysts are not able to identify the origins of the attack.

An important message to come from this study is confirmation that cyberspace has circumvented international regulation and the rules of sovereignty.

To complicate matters, the 1995 G-7 conference generated eight core principles meant to guide the harmonisation and interoperability of information systems.[8]

These are:
- Promoting fair competition;
- Encouraging private investment;
- Defining an adaptable regulatory framework; and
- Providing open access to networks;

While:
- Ensuring universal provision of and access to services;
- Promoting equality of opportunity to the citizen;
- Promoting diversity of content, including cultural and linguistic diversity; and
- Recognising the necessity of worldwide cooperation with particular attention to less developed countries.

The means by which these principles are meant to apply to global information infrastructure are:

- Promotion of interconnectivity and interoperability;
- Developing global markets for networks, services and applications;
- Ensuring privacy and data security;
- Protecting intellectual property rights;
- Cooperating in R&D and in the development of new applications; and
- Monitoring the social and societal implications of the information society.

Conflict emerges when open networks and citizens' access are encouraged, yet intellectual property and privacy are protected by encryption or censorship, resulting in systems islands.

To facilitate interoperability at the governmental level municipal legislators may create regimes which include mandatory encryption or even demand that manufacturers include "trap doors" in their software enabling government agencies to observe electronic systems use. The difficulty arising from this exercise of governmental power is one of proportionality; is the loss of private rights, due to an exercise of parliamentary power, in proportion with legislative purpose? The borderless nature of cyberspace may exacerbate any imbalance by creating an unavoidable extraterritorial impact.

It is possible, however, that cyberspace may not be a common battlefield, but may be simply a conduit for the many forms of IW. Warring actors who are not operating under a common understanding of IW may never meet on a common battlefield. Assorted hacker attacks from various regions of cyberspace may rival terrorist attacks, but this activity may not necessarily be war if it lacks political motivation and purpose. Even so, hacker warfare is necessary, particularly if defensive, as it strengthens network security. In this way, non-public actors are held responsible for their own security and collectively create national security.

CONCLUSION

Cyberspace has, and continues to alter, the environment in which nation states communicate by making the means of international interactions available to individuals. While the Westphalian state-based system of international law remains preoccupied with sovereignty, individuals are creating a meta-jurisdictional electronic society. The difficulty exists in establishing a public international law regime which operates effectively in cyberspace. Although cyberspace may not necessarily be inimical to legal regulation, the absence of geopolitical boundaries and the lack of tangible manifestations of the information contained in cyberspace aid cybercitizens to elude detection and regulation. Further, the boundary-less nature of the Internet requires a new definition of what may constitute an act, or threat, of force.

Traditional notions of force, threats, and use of armed attacks, are defined with respect to physical manifestations, but in cyberspace the concern is the consequences of an attack rather than its nature. Traditionally minded members of the military do not believe warfare will become a video game without physical results, and any IW attacks without physical military backup may be only paper tigers. Even so, cyberspace remains a great equaliser through the deconstruction of social and legal boundaries. Inevitably, the redefinition of traditional notions of sovereignty and warfare will impose a new balance on the public/private divide. This new balance must include greater responsibility for individuals to participate in a growing electronic community. Failure to acknowledge individuals' access to cyberweaponry will inhibit the adoption of public international law rules in the electronic environment.

1 URL:http://www/pyscom.net/iwar.1.html

2 *Ibid*

3 "A Theory of Information Warfare: Preparing for 2020", URL: http/www/cdsar.af.mil/apj/szfran/html

4 J. Arquilla and D. Ronfeldt, "Cyberwar and Netwar: New Modes, Old Concepts, of Conflict", URL: http://www.rand.org/publications/RRR/RRR/fall95.cyber/cyberwar.html

5 *Ibid*

6 *Ibid*

7 "Information Warfare: A Two Edged Sword" URL: http://www.rand.org/publications/RRR/RRR.fall95.cyber/infor_war.html

8 "G-7 Ministerial Conference on the Information Society: Theme Paper" Brussels, 27 January 1995 URL: http://www.ispo.cec.be/g7/keydocs/themepap.html

Tanya Ross-Gadsden is an Associate at the Sydney Office of Allen Allen & Hemsley