

# Information Warfare and International Security

## Table of Contents

Introduction	2
What is Information Warfare and its historical background?	3
Definition	
Historical Background	
What is the relationship between terrorism and Information Warfare?	4
Defining the Threat	4
What is the current international law in regards to Information Warfare?	5
Opportunities	6
Writing International Law	
Creation of a new Organization in the UN Anti-Terrorist Org	
Barriers	7-8
Redefining current International Law	
Intelligence Cooperation	
What is needed to respond to an act of Information Warfare?	8-9
Awareness	
Networks Against Networks	
Classification on Counter-Terrorism Measures	
Conclusion	9-10
References	11

## **Introduction:**

Technology has become more advanced in the last three decades than in the entire twentieth century. The digital future is truly a realistic anticipation. We live in an age where we can create human body parts through simulated DNA to repair broken ones. However the same scientists that make and extend life also create computers that have greater brain power than humans, which can ultimately destroy humankind. There are many different levels of technology, and innovation is always welcome to make the world a more advanced place, however, must we stop for a second to ask ourselves, are we really moving in the right direction? Aren't there always going to be people and groups who will want to sustain the natural way of life without playing God? Whose duty is it to safeguard all the world's citizens who want to live in this revolving world? Today, in the dawn of the twenty-first century, governments across the world face questions like these every day, and in order to cope with them, they come together in the United Nations to offer hope and answers.

Information warfare is a dangerous form of terrorism that threatens trans-continental states, globalized businesses and the human right to free thought. Information Warfare is a dangerous result of technology put into the hands of anybody who wants to weaken another entity. First and foremost, defining Information Warfare is difficult. There are many individuals, organizations, governments and States that have attempted to define information warfare but have always found themselves limiting their boundaries. Therefore, for the sake of definition, I will use the Institute for the Advanced Study of Information Warfare (IASIW) to create a better understanding:

Information warfare is the offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy, an adversary's information, information-based processes, information systems, and computer-based networks while protecting one's own. Such actions are designed to achieve advantages over military or business adversaries.<sup>1</sup>

This definition allows the reader to understand the different aspects that Information Warfare encompasses in hopes that the reader also does not limit the concept. I attempt to answer succinctly several questions about Information Warfare (IW) leading to the main question about the future of IW and what the opportunities and barriers are to combating IW safely. More importantly, I ask, if any State is equipped to react against a major act of Information Warfare in the near future? This paper hopes to explain what IW is, where IW came from, how it threatens boundlessly and why groups attempt to commit acts of IW concluding that States are not sufficiently prepared to react against a major act of IW.

---

<sup>1</sup> Goldberg, Dr. Ivan. Institute for the Advanced Study of Information Warfare (IASIW). <http://www.psycom.net/iwar.1.html>

## What is Information Warfare and its historical background?

In the new post-Cold War period, Information Warfare has taken its place in the era of national security. Although Information Warfare is spoken about at the kitchen table across the globe, Information Warfare remains an indefinite and elusive concept that has been used in an array of contexts. Nevertheless, the definition of IW has remained largely undefined. It is important to stress that although there are multiple definitions of IW, all have some common themes. According to The Terrorism Research Group in cooperation with Georgetown University, Information Warfare will always be evolving and changing its face through time.<sup>2</sup> The group dictates that the success in future wars will depend upon IW. Subsequently, IW can be conducted without the usual expenses of a traditional war waged by individuals, groups or States. Consequently, the State is unprepared for a full-blown act of IW. Dr. Ivan Goldberg, a psychiatrist and clinical psychopharmacologist in New York City and Director of the Institute for the Advanced Study of Information Warfare (IASIW) has defined information warfare that is widely used in the academic and political realms.<sup>1</sup> In Goldberg's definition, the tactic of war has not severely changed, only the standard has changed. His definition is written in the Introduction. In its broadest sense, IW involves the struggling conflict in the communication process. Recently, the increasing use of technology and its significance in today's society has revolutionized the communication process as well as the implications of what Information Warfare entails. Information Warfare has found its roots in the mid-twentieth century when technology advanced during World War II.

Dating back to the first wars, information has played a major role in warfare. The historical background of Information Warfare takes flight with the encryption device used in Germany in World War II called the Enigma machine. Used to encipher messages to troops, the Allies were able to defeat the Germans by deciphering the Enigma code by way of offensive measures of IW. This proved to be very beneficial to the Allied victory in World War II. Furthermore, the Gulf War in the early 1990's marked a crucial moment in the use of IW as a key to its victory on the front lines. Military and commercial use of satellite communications, navigations, surveillances and intelligences gave advantages to the United States of America and her allies over Iraqi forces. Here, the lack of defensive measures of IW proved to be a key factor in defeating the Iraqis.<sup>3</sup> More currently, cyber-warriors, or hackers, increased activity twenty fold between American and Chinese websites after an emergency landing of a recon flight on a Chinese island, causing hundreds of attacks on websites in each rival country. Chris Rouland, of Internet Security System's X-Force, was quoted to NewsFactor as saying, "that there are now 40 to 50 attacks on Chinese and American Web sites per day by hackers in opposing countries, versus one or two per day before the spy plane incident."<sup>4</sup>

---

<sup>2</sup> The Terrorism Research Center in cooperation with Georgetown University. The Terrorism Research Center. [www.terrorism.com/iwdb](http://www.terrorism.com/iwdb)

<sup>1</sup> [www.psycom.net/ikg9.html](http://www.psycom.net/ikg9.html)

<sup>3</sup> - Hrovat, Eric. Information Warfare: The Unconventional Art In A Digital World. Sans Institute, June 30, 2001. <http://rr.sans.org/infowar/infowar.php>

<sup>4</sup> Sausner, Rebecca. NewsFactor Network. U.S., Chinese Hackers Wage Quiet War. April 24, 2001. <http://www.newsfactor.com/perl/story/9203.html>

This even proceeded after the US bombed the Chinese embassy in Kosovo in May 1999 and as a result, government sites were immobile for days by Chinese hackers. As nation-based cyber systems are increasingly complex, more involved roles in international business, daily life and national defense, these computer networks have become more exposed to transnational threats.<sup>5</sup>

### **What is the link between terrorism and Information Warfare?**

There is a distinctive link between terrorism and Information Warfare. Information Warfare, as a form of terrorism, appeals to its perpetrators for several reasons. Terrorism appeals as a weapon of the weak in an obscure way to pursue war by attacking disproportionately to impair and try to defeat an allegedly superior force. Subsequently, terrorism is an attractive way to assert identity and command attention. Consequently, terrorism is a way to achieve a new future order by deliberately destroying the present.<sup>6</sup> A blend of all of these motivations will endure in the information age. “However, terrorism is not a fixed phenomenon: its perpetrators adapt it to suit their times and situations. What changes is the conduct of terrorism – the operational characteristics built around the motivations and rationales.”<sup>6</sup> According to Arquilla, Ronfeldt and Zanini, there is a change in organization, doctrine, strategy and technology in Information Warfare. Primarily, groups of terrorists will move from hierarchical towards network designs. These groups will surpass State borders to trans-continental orders. Furthermore, information terrorists will likely acquire new capacities for lethal acts, focusing towards a “war paradigm”. They may participate in acts of social disruption as well as target disruption, needing States to restructure their approach to a doctrine and strategy that is more effective. In addition, information terrorists are more likely to use advanced information technologies for defensive and offensive purposes. All of these reasons lead to the belief that terrorism is developing in a trend called netwar.

### **Defining the Threat:**

In the beginning of the twenty-first century, the world found itself in a privileged position in technology and cyber-technologies. The use of the Internet and cyber-systems has brought not only advances in the quality of life, but also new threats to the international community. The more advanced interconnectivity technology becomes, the more complex international commerce endures. According to Joyner & Lotrointe, massive computer networks provide multiple links between and among systems that, if not properly secured, can be operated from isolated locations to gain illicit access to data and operations in other systems.<sup>7</sup> The consequential damage can vary, depending on the type and extent of the IW threat. Western societies are the greatest at risk; similarly the intelligence community is seriously concerned. Industries that benefit from cyber-technological advances could be defenseless if important networks providing power, transportation, national defense and medical services are violated and damaged. The

<sup>5</sup> See Defense Science Board Task Force, *Information Warfare: Defense (IW-D)* Nov. 1996 2 15.

<sup>6</sup> Arquilla J., Ronfeldt D., Zanini M. *Networks, Netwar, and Information-Age Terrorism*. Rand Publications, 1999. Chapt. 4

<sup>6</sup> Arquilla, Ronfeldt, Zanini. P 76

<sup>7</sup> Joyner C., Lotrointe C. *Information warfare as International Coercion: Elements of a legal framework*. *European Journal of International Law*, Vol. 12, No. 5, 2001, pp. 825-866.

pervasive nature of cyber-based IW bestows new international military repercussions, and provokes additional critical concerns of where IW fits into the current body of contemporary international legal rules pertaining to the use of force.<sup>7</sup>

### **What is the current international law in regards to info warfare?**

Worldwide interconnectivity through immense computer networks now makes states vulnerable to new threats. Joyner & Lotrointe believe that international law is likely to rely on UN Charter principles to define the legal boundaries of cyberspace. They also provide that there is a need for modern international law to define more precisely the criteria used to distinguish which state actions are permissible as normal computer-generated transborder data flow from those cyber-activities that might qualify as an act of Information Warfare. Technological change may even reveal contradictions among existing legal principles.

There are many challenges that existing international law does not cover Information Warfare. First, the type of damage that such attacks may cause may be rationally different from the kind of physical damage caused by traditional warfare. Bombs and bullets are visually destructive, however, the disruption of information systems may cause intangible damage, such as disruption of civil society or government services. Secondly, the sovereignty of states is disrupted by the ability of technology to run transborderly. Sovereignty, a fundamental principle of international law since the Treaty of Westphalia of 1648, holds that each nation has exclusive authority over events within its borders.<sup>8</sup> Signals are passed daily across international networks through radio waves or satellite signals, allowing individuals or groups to affect systems across the globe, while national legal authority generally stops at those same borders. Furthermore, the intangible violation of borders that signals may cause may not be understood as traditional violations in a military attack. Third, just how information warfare attacks may be difficult to define as “peace” or “war,” it may be harder to define their targets as military or civilian. In addition, the intangible damage the attacks cause may not be the sort of injuries against which the humanitarian law of war is designed to protect noncombatants.<sup>9</sup> The lack of coherent and cohesive international law regarding information technology does not mean that acts of Information Warfare are not addressed in the courtrooms, rather, it leaves space for many types of Information Warfare techniques to be determined, which can be very dangerous.

The Information Age promises profound change in the future emitting the need for greater international laws to protect civilians from acts of warfare. There are great opportunities in protecting civilians and governments against acts of Information Warfare in the future that must be addressed today.

---

<sup>7</sup> Joyner & Lotrointe p. 831.

<sup>8</sup> Mark W. Janis, *An Introduction to International Law* 1 (2d ed. 1993)

<sup>9</sup> Greenberg, Lawrence & Goodman, Seymour & Soo Hoo, Kevin. *Information Warfare and International Law*. [www.dodccrp.org/iwilindex.htm](http://www.dodccrp.org/iwilindex.htm)

## Opportunities:

For the interconnected global community to prepare for a cyber-based future, questions pertaining to international law must be addressed. New technologies generate new opportunities.<sup>7</sup>

Paradoxically, greater dependence upon new technologies also breeds enhanced vulnerabilities for technologically advanced societies. To exploit vulnerabilities in information resources, more sophisticated tools are becoming available. For these reasons, IW must be regarded seriously – not merely to know when a cyber-based attack might occur, but more critically to know how to react if such an information attack does occur.<sup>7</sup>

According to Joyner & Lotrointe, the large extent of advanced military technologies and the new ways in which they affect states are labeled ‘Information Operations’ within IW is considered a subset. These Information Operations provide logisticians with the ability to know what weapons are in their inventories and where to focus attention, as well as the information necessary to know where a target is, its defenses and how to destroy it. Future international law must adapt to the fast changing nature of transnational communications systems. The growing weapons of Information Warfare are expanding, like a ‘sniffer’ and ‘logic bomb’ or a ‘computer worm’. The disparity between effective international law and cyber-technology has been highlighted in recent events and suggest serious considerations need to be made for a transnational force. Recent events include projects known as Operation Solar Sunrise, Moonlight Maze and the Kosovo Crisis.<sup>7</sup>

The United Nations has an opportunity to focus on not only creating international law regarding Information Warfare but also an organization that focuses on the issues, threats and problems IW poses on the global community as well as a taskforce to address perpetrators. The United Nations has consistently addressed the problem of terrorism, taking both legal and political steps.

United Nations specialized agencies have developed a network of international agreements that constitute the basic legal instruments against terrorism, including the Convention on Offenses and Certain Other Acts Committed on Board Aircraft in 1963, the Convention on the Physical Protection of Nuclear Material in 1980, and the Convention on the Marking of Past Explosives for the Purpose of Detection in 1991. In addition, conventions have been organized including the International Convention for the Suppression of Terrorist Bombings in 1997 and the International Convention for the Suppression of the Financing of Terrorism in 1999. However, none of these agreements address the sole issue of Information Warfare directly.

Politically, the United Nations has supported documents like the Declaration on Measures to Eliminate Terrorism, which has mentioned Information Warfare but does little to deter it. At the moment, Information Warfare is not being addressed by the international community and rather only on the domestic level of States. Thus, the United Nations has not addressed this modern issue to the proper attention it deserves.

---

<sup>7</sup> Joyner & Lotrointe p 830.

<sup>7</sup> Joyner & Lotrointe pp 846-850

Since there is an organization within the United Nations that focuses on terrorism, there should be another organization that focuses on digital terrorism, although these two are inextricably linked, they pose different threats and have different roots. The United Nations may be the only international power that can demand the type of intelligence and cooperation that would be in the interests of all of its State participants, as few States want digital terrorists in their territory. Under UN pretense, this committee would need a taskforce to preempt and react to crimes of Information Warfare. This too is an opportunity for the international community to address before a major act of IW occurs. The creation of a unified body to emit this transnational force has been a highlighted topic amongst many military leaders, government officials and scientists alike.

These are some opportunities that the international community has voiced out as methods in which to address the growing issue of Information Warfare in fear of an attack or as security precautions. However, the same opportunities that can assist Information Warfare in the future can also have negative effects towards the progression of combating IW.

### **Barriers:**

Existing international law regarding Information Warfare is sparse, however, criminal acts of IW are held under laws that are more general and are often open for interpretation. One of the barriers towards safeguarding Information Warfare and protecting citizens from acts of IW is how current international law limits the use of force against perpetrators. According to the Report of the International Law Commission to the General Assembly, UN charter law “clearly prohibits international intervention through the use of armed force, but withholds comments on other, more subtle forms of ‘subversive’ coercion that do not involve, at the very least, a perceived threat of force.”<sup>10</sup> Force is too loosely defined and often instruments vehemently confirm that the prevention against intervention by one state into the affairs of other states, and make relevant the need to devise legal restrictions on the use of cyber-force.<sup>7</sup> Actually, under current international law, it may be inferred then that transnational cyberspace activities that affect the domestic affairs of a state might well breach general legal principles upholding respect for sovereignty and non-intervention.<sup>7</sup> This consideration is a serious barrier to the progression of protecting citizens and States from acts of Information Warfare, and as long as it stands, cyber-activities will continue to put states in breach of UN resolutions that are meant to protect states from traditional uses of force.

Besides the current international law being a barrier towards progression in IW, there are additional problems between states that need to be rectified or overcome.

In order for the United Nations to deal with problems of Information Warfare, states need to learn how to trust each other with intelligence information, especially in Western societies where cyber-crime is the most prevalent. This is a growing problem as

---

<sup>10</sup> While some have attempted to classify covert action as a form of aggression, see Report of the International Law Commission to the General Assembly, *2 Yearbook of the International Law Commission* (1950) 123, at 123-133, UN Doc A/CN.4/SER.A.

<sup>7</sup> Joyner & Lotrointe p 854.

<sup>7</sup> Joyner & Lotrointe p 858

separate states take it upon themselves to invest in private intelligence teams. The intelligence community of the US government recently confirmed that its budget -- kept secret as classified information in 50 previous years since its inception -- totaled \$26.6 billion dollars last year.<sup>11</sup> Paradoxically, the need to share information pertaining to issues of privacy and security are not collectively being achieved. There is historical evidence of states not divulging all intelligence information as well as rivalries between states that choose not to share sensitive information. This further hinders the development of combating IW. "Threats to the United States today are more diverse and dispersed — distributed, if you will — and intelligence priorities shift continuously — presenting a tougher and enduring environment for both collection and analysis."<sup>12</sup> The United Nations also shares its opinion about intelligence. In order for any resolutions to pass through the Security Council, intelligence is the key element that binds states together. Without intelligence, information would not be cohesive, with a certain amount of trust that is invested in each resolution. Furthermore, the UN would like to see efforts made by states to utilize their departments, organizations and personnel to enhance greater trust and build greater intelligence programs to improve methods of reaction, especially outlined in their UN Terrorism Prevention Branch.<sup>13</sup> Overall, the need for greater cooperation in the international community is growing more than ever. Globalization has many benefits that individuals reap, however it also brings many forms of corruption. Intelligence allows those forms of corruption to be exposed while both state governments and international community can then identify the rational behind the perpetrators mission.

### **What is needed to respond to an act of Information Warfare?**

The first step for any effective response is to establish an awareness of the problems enormity to all branches of society. The United States has gone so far as to enact Presidential Decision Directive 63 entitled 'Critical Infrastructure Protection' under President Clinton's Administration calling for a national effort to ensure the security of increasingly vulnerable and interconnected infrastructures in the US, between the government and private sectors and international community.<sup>7</sup> Furthermore, the response to an act of Information Warfare is unique because it calls upon the need for specific action. Each act of crime is individual, however, all require personnel with technical and technological advanced educations and therefore, a response needs the same criteria. Arquilla, Ronfeldt and Zanini offer this type of response.

Given the prospect of a netwar oriented shift in which some terrorists pursue a war paradigm, we then focus on the implications such a development may have for the US military. We use these insights to consider defensive antiterrorist measures, as well as proactive counterterrorist strategies. We propose that a key to

---

<sup>11</sup> Martin, Frederick Thomas. The Future of Information Management in the U.S. Intelligence Community. [http://fc.vdu.lt/Conferences/INET98/3c/3c\\_4.htm#s17](http://fc.vdu.lt/Conferences/INET98/3c/3c_4.htm#s17)

<sup>12</sup>Gannon, John C. Remarks made in regards to The CIA in the New World Order: Intelligence Challenges Through 2015. [http://www.cia.gov/cia/public\\_affairs/speeches/archives/2000/dci\\_speech\\_020200smithson.html](http://www.cia.gov/cia/public_affairs/speeches/archives/2000/dci_speech_020200smithson.html)

<sup>13</sup> United Nations Office on Drugs and Crime. Comments concerning measures for counter-terrorism. <http://www.undcp.org/odccp/terrorism.html>

<sup>7</sup> Joyner & Lotrointe p 836

coping with information age terrorism will be the creation of interorganizational networks within the US military and government, party on the grounds that it takes networks to fight networks.<sup>6</sup>

Networks come in many forms- from government officials to high-tech scientists, all of which contribute their special knowledge to a greater cause.

In addition to creating networks, the United Nations has outlined a classification on counter-terrorism measures in the Office of Drugs and Crimes. This classification breaks down over eight categories how to address acts of terrorism, from: political and governance policies, economic and social policies, psychological-communicational-educational expressions, military efforts, judicial and legal efforts, police and prison systems, intelligence and secret services and other measures of support offered to respond to an act of terrorism. Although IW is not a traditional form of terrorism, often, similar methods of reaction can be effective. Lastly, without having to say, enhancing security systems is a mandatory step towards greater security, however is not an absolute end to forms of Information Warfare.

### **Conclusion:**

In light of this research, I conclude that a State is not equipped to react against a serious act of Information Warfare. By the very definition of Information Warfare, acts of crime are committed without regard to state boundaries and national sovereignty. In conjunction with the high-tech nature of these crimes and lack of international law specifically punishing perpetrators who commit these crimes, States have no precedent in which to use for justification. A State will have to create a program from scratch, on highly advanced and often classified information on cases that have the ability to be as different as black and white, yet all call for the need for sufficient research, intelligence and taskforces like how traditional forms of terrorism encompass. The sheer mass of this project becomes so immense that often States lack funding, support and personnel who can truly and profoundly understand the type of devotion that is needed. In addition, the bureaucratic machines that create research teams, intelligence hookups and reactionary taskforces can hold back meaningful projects by withholding funding, lack of glorification by the issue (i.e.: the non-sexiness of a crisis in the infrastructure trafficking system v. the sheer magnitude importance of it) and the inefficiency that government endures.

Information Warfare is a fairly recent form of terrorism that although has played an important role historically throughout wars, has taken new shapes over the last few decades as technology has become so advanced. The relationship between terrorism and Information Warfare is also only known to a certain group of people in society who actually understand the logistics of what Information Warfare is. There is no comparison to the population throughout this world who can recognize acts of terrorism, however, do not understand the theory of Information Warfare nor its boundaries. This is from the lack of awareness of the world's citizens as well as a failure of national governments to inform their citizens of this highly dangerous form of terrorism. Defining the threat of Information Warfare is something that can never be fully detailed since acts of IW are distinct from each other. Most importantly, the current international law is hindering the

---

<sup>6</sup> Arquilla, Ronfeldt, Zanini. p 77

future of International Warfare. It creates both opportunities for change however barriers change because of interconnected laws that need to be further detailed. Beyond international law, there are other opportunities and barriers for combating IW for states and non-state entities. There are several efforts that can be made to respond to an act of Information Warfare, however, they are new and sparse around the world and are ineffectively spread out. All of these obstacles impede the future of Information Warfare for the benefit of humanity. Although most Western societies live in an environment that is highly technologically advanced, it is often within small circles that this technology is fully understood. That often means that a few people could run society who understand the capacities the entire State can endure. Until State governments catch up with the level of technology that the private sector capacitates, it will be very difficult for that same State to react against an act of Information Warfare, and until State governments realize the need for a truly international cooperation, Information Warfare will continue to have strange boundaries that many international lawyers, politicians and citizens that will not be able to distinguish.

## References

1. Arquilla, J., Ronfeldt, D. "Cyberwar is Coming!" *Comparative Strategy*. Vol. 12 No. 2 Summer 1993. pp.141-160.
2. Denning, Dorothy E. "Is Cyber Terror Next?" *Social Science Research Council*, Nov. 1, 2001.
3. Molander, Roger C., Riddile, Andrew S., Wilson, Peter A. *Strategic Information Warfare: A New Face of War*. 1996.  
<http://www.rand.org/publications/MR/MR661/> Dec. 4, 2002.
4. Nacos, Brigitte. *Terrorism and the Media*. New York: Columbia University Press, 1996.
5. Reardon, Thomas M. "Information Warfare: Protecting Force Sustainment." *Military Intelligence Professional Bulletin*.  
<http://www.fas.org/irp/agency/army/tradoc/usaic/mipb/1997-1/reardon.htm>
6. Strassmann, Paul. *Govt. should blaze global information warfare trails*. Aug. 8, 2001. <http://www.strassmann.com/pubs/searchsecurity/2001-8.php> Dec. 4, 2002.