



DND Photo AEC98-46

A Canadian Forces CC-130 *Hercules* transport deploys an impressive array of decoy IR flares from its self-protection suite.

## APPLYING ELECTRONIC WARFARE SOLUTIONS TO NETWORK SECURITY

by Major Ron Smith and Dr. Scott Knight

### Introduction

The militarization of space has garnered much public attention in recent years. Many past and current space programmes have been influenced by defence-related research and military space-system deployments (i.e., sensors), and, therefore, the military usage of space really should not surprise anyone. Advocates against weaponization of space may hold out hope that the current thin public and governmental support for space-based defence systems will not last long enough to field such systems; others may conclude that such weapons are inevitable.

The militarization of the Internet is the subject of similar debate. The Internet has its foundations in defence research and is literally an extension of a once solely military ‘internetwork,’ so to speak [1]. Despite the numerous and well-published vulnerabilities of ‘open’ computer networks, the military use of the Internet is widespread, and it is aggressively expanding. Despite its history and despite its widespread military use, the Internet might not be viewed by the public as a piece of strategic military infrastructure. However, the public today has come to rely on it and would likely see the Internet as a system that must be protected. The weaponization of the Internet is a different issue – one

that many might not have seriously considered. Again, advocates for ‘peaceful’ use of the Internet might contend that there is no justification or support for such aggressive measures, while others might conclude that it is inevitable. In fact, conflict on the Internet has already begun. Consider the use of targeted distributed denial-of-service attacks against commercial and political targets. In Lieutenant Colonel Lionel D. Alford’s paper on Cyber Warfare [2], it is apparent that the military is only too aware of the potential for nations to be engaged in “warfare without violence” through the vulnerabilities of software – intensive systems. So many strategic software – intensive systems<sup>1</sup> are accessible through computer networks it seems inevitable that disruptive and destructive attacks by computer network weapons will one day be delivered via the Internet. National security agencies also have the weaponization of the Internet on their radar screens [3,4].

---

Ron Smith is an Assistant Professor in the Electrical and Computer Engineering Department at RMC, where he is also a PhD student pursuing studies in computer network security. Scott Knight is an Associate Professor in the Electrical and Computer Engineering Department at RMC, and is the lead researcher of the Computer Security library.



As a further example of a host platform for EW jamming/deception systems employed in recent decades, the Canadian destroyer *HMCS Algonquin* carries the SLQ-501 Canadian Naval Electronic Warfare System (CANEWS), the SLQ-503 jammer and the SLQ-25 *Nixie* torpedo deception system, as well as four 6-barrelled Plessy *Shield IR*/chaff dispensers and the *Nulka* hovering decoy system.

The aim of this article is to explore the Internet as a theatre of Information Operations and to draw lessons from Electronic Warfare (EW), a more mature branch of Information Operations. It will focus primarily on a military perspective for computer network security.<sup>2</sup> It is proposed that the term computer network warfare (CNW) be used as an umbrella term for computer network disciplines much like that of EW. It also proposes that the various computer network-related doctrines be realigned under a CNW doctrine, and that there be parallels with that of EW doctrine where it is appropriate. Systems that must ultimately implement the operations of CNW must be reassessed in light of the existing and more mature systems used in implementing EW operations. A case study for one category of CNW system is presented to illustrate how this comparison with EW can provide new insights into the CNW space.

An invasion into a nation’s perceived electromagnetic (EM) space is treated as an aggressive act, and is countered according to war and peacetime proven doctrines of EW. US Joint Publications define an electronic attack to include “actions taken to prevent or reduce an enemy’s effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception... [5]”. The name given to measures used to control and protect the EM spectrum clearly includes the word warfare. There is no mistaking the classification of related doctrine;

it consists of acts of war. An invasion into a nation’s perceived computer network (CN) space should also be treated as an aggressive act, and it should be countered according to a proven doctrine of Computer Network Warfare. US Joint Publications define a computer network attack (CNA) to include “operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves [6].” However, the name afforded to the measures used to control and protect the computer network space does not include warfare. The current terminology and doctrine refer to computer network security, but it is difficult to know whether a computer network attack is an act of war or a criminal act, and yet, the correct and legitimate response depends upon making this distinction. A nation’s computer network space is a critical part of its commercial, civil and military space, just as is its electromagnetic

space. An intrusion into this space can have grave consequences, and, in this way, it is no different than any other type of invasion. It is an aggressive act. In some circumstances, it is an act of war, and it demands an appropriate response.

**“An invasion into a nation’s perceived electromagnetic (EM) space is treated as an aggressive act, and is countered according to war and peacetime proven doctrines of EW.”**

### Motivation

Investigating the parallels between EW and CNW reveals a striking degree of similarity between the disciplines on a number of levels. For example, the control and use of the CN spectrum<sup>3</sup> can be described and discussed in much the

same way as the control and use of the EM spectrum, and both already fit under the doctrine of Information Operations. Both computer network intrusion detection systems (IDS) and EW detection systems rely on the concept of threat libraries and attack signatures containing data, which is often collected through separate out-of-band means. Also, as the probability of detection of a target increases, so does the probability of false positives, and this holds for both IDS and EW systems.

**“While all of EW fits as one capability defined under the IO umbrella, the same cannot be said for computer or computer network capabilities.”**

The history of EW is decades older, and the associated doctrine and systems are much more mature. The whole nature of the measures/countermeasures cycle in EW is several generations of research and systems old; the measures/countermeasures cycle in CNW is barely in its infancy. By tapping into the lessons learned in EW, we may be able accelerate our progress in CNW. These observations have also gone largely unrecognized in terms of terminology, doctrine and systems development.

Identifying and then acting upon opportunities to realign the terminology and the doctrine of the two fields could have wide-ranging benefits. Personnel already trained in one discipline could more quickly train in the other. Commanders and senior military/government officials, who have lived with and understand the operations of EW, might more easily apply their intuitions to the newer discipline.

### Comparing Electronic Warfare to Computer Network Warfare

*Electronic warfare operates within a strategic medium that defies geographic boundaries. So too does computer network warfare.*

We will begin this section of the article by reviewing some of the basic definitions covering the two disciplines. Similarities between the doctrine used to guide EW and CNW operations are presented. Finally, specific parallels between the weapon systems used in the implementation of both types of warfare are identified. The primary source of material for this section is US Joint Publications for Information Operations (IO) and EW [5,6].

In the military context, “EW refers to any action involving the use of EM or directed energy to control the EM spectrum or to attack the enemy [5]”. EW is traditionally subdivided along the lines of electronic support and countermeasures. In current doctrinal terminology, these divisions include electronic attack (EA), electronic protection (EP) and electronic support (ES). Some may be more familiar with these using older terminologies under the respective headings of electronic countermeasures (ECM), electronic counter-countermeasures (ECCM) and electronic warfare support measures (ESM).

From a doctrinal perspective, EW sits as a top-level capability under the IO umbrella. EA, EP, and ES provide a separation of capabilities and activities within EW, with each of the three further subdivided into differing types of activities. EA consists of non-destructive jamming and deception as well as destructive EM and directed energy weapons. EP includes passive and active means of frequency deconfliction, protection from enemy and friendly EW,

EW reprogramming and electronic masking. ES divides into threat warning, direction finding and collection in support of EW. Division along the lines of offensive versus defensive usage is not identified at any EW level, and is only addressed in the broader IO context within which EW is employed. The terms offence and defence relate to the mission objective rather than the capability or activity being performed. This doctrine has evolved out of decades of field experience, and one could argue that it is proven relatively sound through the consistent and overwhelming control of the EM spectrum enjoyed by US forces in the battles of the past decade, particularly when used in support of gaining air supremacy.

Some of the more traditional systems that fall out of the EW doctrine are identified next. They are categorized according to EA, EP and ES applicability, and are drawn from radar band systems.<sup>4</sup> Typical EA implementations include various types and bands of jammers. Systems used in EP operations are perhaps the more difficult to identify. Many systems used in support of EA may also be used in EP, with perhaps some modification to configuration or usage. Examples include the use of an ECM system in an escort jammer, or the use of a jammer programmed with techniques to counter an opponent’s jamming, which is traditional ECCM. EP also includes such systems as chaff and flare dispensers, identification friend or foe (IFF), towed or unmanned decoys, and stealth weapon system platform designs. ES systems range from pure warning devices, such as radar warning receivers (RWR), to pure collection systems, such as electronic intelligence (ELINT) recorders. Somewhere in between lies a more interesting implementation, the electronic support measures (ESM) system – a system responsible for the collection, identification and location (usually) of EM signals of interest. An ESM system usually works in conjunction with EA and EP systems to form a cohesive EW suite.

By contrast, the terminology associated with military computer network operations is not straightforward. As the discipline is new and still very fluid, the terminology can be inconsistent across publications and often also within the same publication. Information Warfare (IW) is a popular term but it is much broader than just CN operations, and it usually includes other information-oriented operations such as EW and psychological operations. The terms ‘Cyberwar’ or ‘Cyberwarfare’ are also popular, and, again, they are used with mixed meaning. In some contexts [7], they are



A now-retired Canadian Forces CT-33 on an air defence exercise. It carries a full suite of electronic jammers and chaff/flare dispensers.

used almost interchangeably with IW, including a wide range of operations against information and communication systems. In other contexts [2], they refer more specifically to operations targeted against software intensive systems. This list goes on and includes terms such as Command and Control Warfare, Network-Centric Warfare, 'Netwar' and 'Hacker' warfare. While each may contribute to, or contain, computer network operations, none of them fully or succinctly describe computer network operations in the military context. In the context of this article, the term proposed for further dissection and comparison with EW is computer network warfare (CNW). It is defined to include any military operation involving computer network attack (CNA), computer network protection (CNP) and related computer network support (CNS), and it will be further defined here with respect to doctrine.

In military doctrinal terms, CN operations terminology is only slightly more structured than the IW terminology presented above. While all of EW fits as one capability defined under the IO umbrella, the same cannot be said for computer or computer network capabilities. No fewer than five separate capabilities are listed that relate to one or both of these disciplines [6], and currently include computer network attack (CNA), computer network defence (CND) [5], network

management, computer security and information security. The earlier selection of CNW as a top-level capability under the IO umbrella seems to be natural. The existing doctrinal terms CNA and CND fit nicely under CNW and, when so aligned, start to resemble at least the structure of EW doctrine.

With this alignment, identifying the parallels in doctrine between EW and CNW is relatively straightforward. CNA is defined under existing doctrine [6, 8] to include operations "to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves" and is a close parallel to EA.<sup>5</sup> The current doctrinal term CND includes "defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction" and compares to EP. To highlight the similarity with EW doctrine, it is proposed that these activities be placed under a subdivision of CNW called computer network protection (CNP), vice CND. This replacement of the term CND by CNP also emphasizes that the terms offence and defence are used more properly when referring to the mission objective, rather than the capability or activity being performed. As with EP, CNP can be used in the offence or defence. A specific comparison to EP then implies that CNP involves passive and active means of network traffic

deconfliction, protection from enemy and friendly CNW, CNW reprogramming<sup>6</sup> and network masking. Network management appears in several Joint Publications as a top-level capability under IO, but it is not clearly defined nor does it appear as an activity separate from CNA and CND. To address this capability deficiency, it is suggested that a new term Computer Network Support (CNS) be defined, and that the activities within it can be structured to parallel ES. Following guidance from this analogy, CNS would include threat warning, direction finding<sup>7</sup> and collection in support of CNW.

Systems or tools that could be used in support of computer network attacks are prolific, and can be found in various texts on computer security or at various ‘hacker’ and security web sites [9, 10]. Collections of such tools organized under an architecture suitable as a CNA weapons system do not yet exist, or, at least, not as published in the unclassified domain. CNP includes systems of protection, such as firewalls, systems of deception, such as honey pots,<sup>8</sup> and honey nets [11], as well as network deconfliction techniques,<sup>9</sup> such as public key infrastructure (PKI) based systems and stealth technologies, such as virtual private networks (VPNs). As is the case with EP, CNP can theoretically include almost any CNA system, only that its use is in a protection versus an attack role. Since no such CNA systems exist, this class of CNP systems is also nonexistent. CNS systems<sup>10</sup> include the most common computer security tools, and, similar to ES, the systems range from pure collection to pure warning system. ‘Sniffers’ and scanners are examples of the former, while most intrusion detection systems (IDS) are illustrations of the latter. The IDS is the more interesting system, capable of both information collection and attack warning.<sup>11</sup>

**“Defence against intelligence gathering ranges from conventional information protection to covert and minimal usage of certain high value capabilities.”**

The parallels between the proposed CNW systems and those of EW are depicted in Table 1. Some CNW systems have a fairly obvious and direct counterpart, while others require more imagination to visualize the similarities. It can be useful to examine these relationships. Consider the ESM to IDS analogy. The similarities between these two systems are quite striking. Each requires considerable in- and out-of-band intelligence data to function properly. Out-of-band data, which characterizes various forms of attack, is contained in an attack signature database.

Each kind of system provides warning of potential and on-going attacks. They also allow the operator to collect data prior to and during attack, often facilitating on-the-fly system reconfiguration. Both support operator-in-the-loop and operator-out-of-the-loop operations. The standard architecture is also very similar, including sensors, analysis engines, data repositories and response modules. It is in this last area where EW and CNW begin to seriously part ways. Most ESM systems are deployed as part of a larger EW package. The package includes EA and EP modules that can be used to direct a wide range of response actions. Similarly then it might be expected that in the CNW theatre, CNA and CNP capabilities would be combined with an IDS. Currently this is not possible because, as noted above, cohesive tool suites do not yet exist. It is proposed that this weapon system be called a *computer network jammer*<sup>12</sup> (CNJ). Specifics of the nature of this weapon will be explored in the next section of this article.

#### A Case Study: Applying EW Countermeasures to CNW

In “Summer Dreams of IDS, [12]” the author envisions a Manhattan Project style initiative to develop an IDS capable of automated responses, such as ‘on-the-fly’ upgrading and tuning of the software applications and

**Proposed EW/CNW Parallel Systems**

Category	Electronic Warfare	Computer Network Warfare
EA/CNA	electronic jammer	<i>computer network jammer</i>
	directed energy weapon	<i>computer network blaster</i>
EP/CNP	electronic jammer	<i>computer network jammer</i>
	chaff/flare dispenser	honey pot
	unmanned decoys	honey net
	identification friend or foe (IFF)	public key infrastructure, firewalls
ES/CNS	stealth platform	virtual private network
	radar warning receiver (RWR)	firewall alarms
	electronic intelligence (ELINT)	sniffer, scanner
	electronic support system (ESM)	intrusion detection system

*Items in italics denote a proposed new system or component.*

Table 1

operating systems of monitored systems, in addition to taking countermeasures against ongoing attacks. The reality of current ID systems is far from this dream. While the common intrusion detection framework (CIDF) standard model of an IDS includes an automated response engine [13], most IDS implementations have very limited response capability, usually ranging from log entries to system alerts in the form of audio, visual, e-mail or pager advisories. A rare few go so far as to dynamically update IDS or firewall filters, while fewer still<sup>13</sup> employ any true sense of active countermeasures. The computer network jammer introduced in the previous section is envisioned to provide this tactical capability. It could be employed in conjunction with an IDS as a stand-alone system, or form the basis of an expanded IDS response module.

Prior to outlining the basic requirements and design of a computer network jammer, it is helpful to review a typical network attack sequence. Since the CNJ is conceived based upon the electronic jammer, it is useful to first review a typical attack sequence employing EW, with particular emphasis on the countermeasures available. Therefore, a typical EW scenario will be presented, followed by a parallel sequence involving a network attack. The requirements of the computer network jammer fall out of this discussion. It is important to note that the attacks are assumed to be taking place during an active military operation involving the use of EW/CN assets, and where policy (law) permits that a force commensurate with that used by an aggressor can be employed.

A significant amount of intelligence information is required in support of EW operations against any specific system – information that can be collected through in- or out-of-band means. For example, an attack planned against a specific radar system may require data such as frequency of operation, pulse width, pulse repetition frequency and associated modes of operation, modulation schemes, and so on. Generally, the more sophisticated the attack, the more detailed, and arguably difficult, the intelligence requirement. Defence against intelligence gathering ranges from conventional information protection to covert and minimal usage of certain high value capabilities. Countermeasures at this strategic level may include self-evaluations to determine that which an enemy is likely to know, or might also include injection of false information into channels suspected of being monitored. Rarely do jammers play any significant role at this stage of protection or countermeasures.

In advance of a conventional weapons attack against forces employing EW assets, the launch of the physical weapon is almost always preceded with a search phase, followed by a track or lock-on phase. It is these two phases of the attack where EW techniques begin to be very useful. In the search phase, an enemy<sup>14</sup> will generally use the EM spectrum to find a target. The EW protection measures available in this phase range from more

costly systems, such as stealth or unmanned decoys, to relatively inexpensive chaff dispensers.<sup>15</sup> The traditional electronic jammer fits somewhere in the middle, providing obscuration techniques, such as spot/barrage noise, pseudo random noise or the generation of multiple false targets.

Progression to the lock-on phase implies that search phase countermeasures were not successful. Despite attempts to make one invisible or hide in the 'noise,' one is still in EM view. This is a significant point in the attack sequence, usually signifying that a physical and potentially lethal attack is imminent and more drastic measures are required. Typical jamming countermeasures include deception techniques, such as repeater delay, random Doppler, and range/velocity gate stealers. The objective is for the attacker to be deceived as to the victim's real position or velocity, and to 'lose lock' and revert to search mode. These observations from the EW theatre will now be applied to study similar issues in a CNW context.

A significant amount of intelligence information is also required in support of CNW operations against any specific system – information that can also be collected through in- or out-of-band means. For example, an attack planned against a specific sub-net may require data, such as the range of Internet protocol (IP) addresses, size of network, ports open<sup>16</sup> and associated services of operation, encryption schemes in use, and so on. Generally, the more sophisticated the attack, the more detailed, and arguably difficult, the intelligence requirement. Defence against CN targeted intelligence-gathering ranges from restrictive firewalls to covert networks, such as private and virtual private networks (VPN). Countermeasures at this strategic level may include self-evaluations to determine what an enemy is likely to know. For example, the use of network vulnerability scanners by the owners of the network is becoming more common as a means of assessing the vulnerabilities of critical networks. Injection of false information into channels suspected of being monitored is also a possible countermeasure – one that is not yet common practice, but, arguably, should be routine. Unlike EW jammers, there is potential for jammers to play a significant role at this stage of protection or countermeasures. Upon detection of network scans, a CNJ might very well be designed to provide deceptive information.

In advance of a computer network attack, the launch of the virtual weapon<sup>17</sup> is almost always preceded with a scan phase followed by an installation phase.<sup>18</sup> As with a conventional attack involving defensive EW assets, it is these two phases of a computer attack where CNW may be very effective. In the scan phase, an enemy will generally use the CN spectrum to locate the target and identify vulnerabilities. Current CNW protection measures available in this phase range from relatively costly solutions, such as stealth (the stealthiest networks being private ones) and restrictive firewalls, to hardened operating systems, to less costly conventional IDS. As noted above, an IDS does not currently offer effective

automated response options and has so far been more successful in recording attacks for post-mortems than in preventing or averting an attack. The proposed CN jammer offers a new solution, again fitting somewhere in the middle of the range of countermeasure options. In this deployment, a CNJ would likely operate in conjunction with an IDS, providing obscuration and deception techniques. Obscuration techniques in CN terms might include such actions as single and multiple port DOS,<sup>19</sup> pseudo-random port DOS, or DDOS directed against the scanning sites. CNJ deception techniques might include such actions as false host responses and false network responses.

Progression from the scan phase to the installation phase implies that vulnerability has been found despite the countermeasures taken. It is also a very critical point in the attack sequence, signifying that a potentially lethal attack<sup>20</sup> is imminent and that drastic measures are required. As with the lock-on phase in the EW scenario, the duration of the installation phase is usually very short, from milliseconds to a few seconds. Countermeasures at

this stage might range from network manoeuvring (disconnection, reconfiguration) to smart deception (honeynets) to rapid counter attack (DOS). Again, a CNJ is envisioned to fit somewhere in the middle, but also to be potentially involved in a more drastic counterattack. A set of deception countermeasure techniques might include repeater facade, random false services and IP/port stealers.<sup>21</sup> The objective is for the attacker to be deceived as to the real location on the net, or the real services provided by the victim host, thus losing 'lock-on' and reverting to scan mode. To summarize, there is a significant amount of similarity between the two scenarios. Figure 1 highlights this similarity from the perspective of the effects of jamming on the attack sequence.

What might a typical computer network jammer look like? It would be a system capable of being employed in both offensive and defensive roles, either alongside an IDS or stand-alone, and either operated from within the defended host or on a standoff support host. It would be a countermeasure device containing a programmable suite of obscuration and deception techniques.

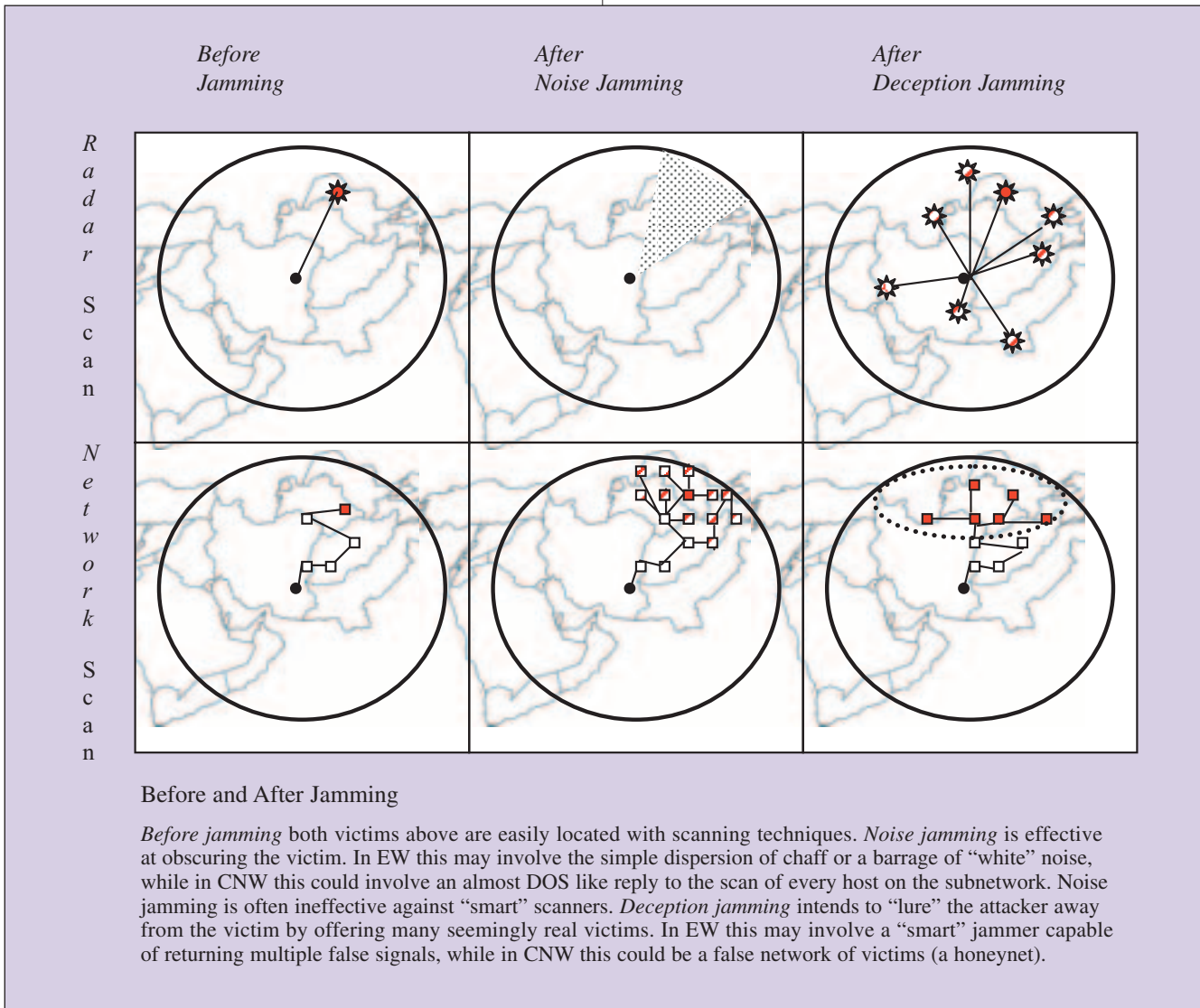


Figure 1

## Electronic versus Proposed Computer Network Countermeasures

EW	CNW	CN Technique Description <i>(if not self-explanatory)</i>
<b>Obscuration</b>		
Stealth	Private networks, VPNs	
Decoys	Honey Nets	
Chaff		
Spot/Barrage Noise	Single/Multiple Port DOS	A denial of service attack directed at single or multiple service ports on a designated host.
Pseudo-random Noise	Pseudo-random Port DOS	A denial of service attack directed at random service ports on a designated host.
Multiple False Targets	DDOS	A distributed DOS attack directed at a designated host.
<b>Deception</b>		
Flares	Honey Pots	
Manoeuvres	Disconnection	
Repeater Delay	Repeater Façade	All expected attack sequence replies are repeated back to the attacker as if the compromise were successful, while future attempts to use the compromise will be traps or faulty services.
Random Doppler	Random False Services	Insertion of random services (active ports) where no real service exists.
Range/Velocity Gate Stealers	IP/Port Stealers	A dynamic re-mapping of an ongoing attack to a non-existent host or honey pot or in the case of a port stealer the dynamic relocation of a legitimate service while the attack proceeds on the now disabled service port.

Table 2

A summary of the types of techniques such a jammer might contain is illustrated in Table 2. Significant research is required to fully define a suite of operational CNJ techniques. Like an IDS, it would require in- and out-of-band intelligence support. Employment of a CNJ as a weapon system would have to be clearly spelled out in new doctrine to be contained under IO within a broader and realigned CNW capability. The bottom line is that the CNJ would be a weapon system introduced as an almost natural response to the reality that war is being waged via computer networks, and it cannot continue unchecked.

### To Jam Or Not To Jam

It would be naïve to think that this is the first time an active or offensive response IDS has been considered. Rebecca Bace [14] describes both passive and active response options, and, for good reasons, she dismisses most active response options as being either impractical or impossible for scientific, tactical or political (read legal) reasons. What this article is saying is that approaching the design of a current CNS component along lines parallel

to its EW counterpart may well lead to previously unimagined and perhaps surprising solutions. The case of conceiving a CNJ fashioned out of the traditional design of an electronic jammer yields a mix of results. Some solutions emerge that are both unique and surprisingly simple – deception techniques being one of them. Other solutions appear as possible but impractical without further supporting technologies or techniques. Counter-DOS may fit this case. Finally, other parallel solutions either have no relevant counterpart or are impossible, given the difference in medium. Directed energy beams certainly appear to fall into this category.

**“Although there are good reasons not to introduce CN jammers... there are compelling arguments for their introduction, and many of the detractors can be challenged.”**

Although there are good reasons not to introduce CN jammers, including the mere fact that they advance the weaponization of the Internet, there are compelling arguments for their introduction, and many of the detractors can be challenged. The three main reasons not to develop the more aggressive IDS responses proposed by the introduction of a CNJ are: 1) The attack might not actually be coming from the indicated source IP, as the host might either be a compromised or spoofed host, and

thus, an innocent victim is countered. 2) The attack may be escalated by the response. 3) The response might result in criminal or civil legal actions. Each of these points has merit. Unrestrained use of CN jamming would wreak havoc on networks, resulting in a loss of capability for all users. However, the same can be said for electronic jamming. An EW electronic attack or active protection and support measures are not entered into lightly, but they are definite force multipliers that have been, and will continue to be, used in warfare. Similarly, CN attacks, as well as active protection and support measures, have a time and place, particularly in military operations. Whether western governments agree to develop them has little bearing on whether they will some day soon exist. Therefore, assume that they will exist and that they will be used, despite the aforementioned concerns. The cycles of measure and counter-measure are now unfolding. The choice is to develop capability or live with increasing vulnerability.

### Conclusion

The EM spectrum is often used in support of a conventional military attack. Similarly, the CN spectrum is often used in support of a computer attack. EW defines the operational capabilities associated with the control and protection of the EM spectrum, and has a well-developed set of battlefield tested doctrine. CNW defines the operational capabilities associated with the control and protection of the CN spectrum, and currently consists of a disjointed set of partially complete doctrines that one could argue is not battlefield tested.

There exist both obvious and not so obvious parallels between the two disciplines, including terminology, doctrine and systems. For example, a review of these parallels at the system level identifies a missing CN weapon – the computer network jammer. As the following quote from Network Magazine columnist Rik Farrow suggests, one need not look to EW to see this omission. "... Intrusion detection systems are a bit like the Star Wars shield – something that does not work. For intrusion detection systems to function correctly, they must detect the attack before it impacts its target, and stop or deflect that attack. [15]"

At the operational level, both EW and CNW require substantial intelligence support to be effective. In defending against conventional attacks, EW countermeasure employment is most effective in the pre-launch search phase. In defending against a computer network attack, CNW countermeasure employment could be equally effective in the pre-launch scan phase if a suitably equipped CNJ were to exist. With some imagination, CNJ obscuration and deception techniques can be envisioned that compare nicely to their EW counterparts.

This article has proposed and demonstrated that there are potential benefits in a realignment of terminology, doctrine and even systems of CNW, based upon the similarities and lessons learned from a more mature discipline – that of electronic warfare. This approach is not a panacea. New solutions will not be found in every comparison, and even when solutions are found, they will not be ready 'out-of-the-box.' Despite the similarities, EW and CNW operate in different mediums under differing laws of physics, technological evolution and politics. Additionally, much research remains to capitalize on even the ideas proposed in this article. They include, but are not limited to, such diverse areas as development of unified CNW doctrine, CNJ 'jamming' techniques, network deconfliction protocols, methods of network direction finding, and methods to identify concealed attacker hosts.

Finally, the debate concerning the weaponization of the Internet is not an easy one. Just because a CNJ can be built does not mean one has to be built. However, it is very compelling to take advantage of some of the countermeasure concepts presented, particularly the deception techniques that just might turn the tables on the network attackers, making them sort through the volumes of false data in search of the true vulnerable machines.

The computer network jammer will not make the Internet a better place to live. However, its existence is inevitable.



## REFERENCES

- [1] Scott Ruthfield, *The Internet's History and Development – From Wartime Tool to the Fish-Cam*, ACM Crossroads, 2.1 September 1995. <<http://www.acm.org/crossroads/xrds2-1/inet-history.html>>, accessed 15 April 2004.
- [2] Lionel D. Alford, *Cyberwarfare: A New Doctrine and Taxonomy*, *Crosstalk*, April 2001.
- [3] Lawrence K. Gershwin, National Intelligence Officer for Science and Technology, Statement for the Record for the Joint Economic Committee, *Cyber Threat Trends and US Network Security*, (as prepared for delivery), 21 June 2001, <[http://www.cia.gov/nic/testimony\\_cyberthreat.html](http://www.cia.gov/nic/testimony_cyberthreat.html)>, accessed 15 April 2004.
- [4] Ochanomizu Associates, *National Security Forum Consortium for Research on Information Security and Policy Center for International Security and Cooperation*, Hoover Institution, Stanford University, 7 December 1999.
- [5] Joint Publication 3-51, *Joint Doctrine for Electronic Warfare*, 7 April 2000.
- [6] Joint Publication 3-13, *Joint Doctrine for Information Operations*, 9 October 1998.
- [7] *Space and Electronic Warfare Lexicon*, <<http://www.sew-lexicon.com/>>, accessed 15 April 2004.
- [8] Joint Publication 1-02, *DOD Dictionary of Military and Associated Terms*, 12 April 2001, as amended through 9 Apr 2002, <<http://www.dtic.mil/doctrine/jel/doddict/data/c/index.html>>, accessed 15 April 2004.
- [9] McClure, Scambray & Kurtz, *Hacking Exposed Network Security Secrets & Solutions* (New York: Osbourne/McGraw-Hill, 1999).
- [10] <<http://www.insecure.org/>>, accessed 15 April 2004.
- [11] Bruce Schneier, *Honeypots and the Honeynet Project*, *Crypto-Gram Newsletter*, 15 June 2001, <<http://www.schneier.com/crypto-gram-0106.html>>, accessed 15 April 2004.
- [12] Rik Farrow, *Summer Dreams of IDS or: Why you can't buy the IDS you've been dreaming about*, Network Defense Column for *Network Magazine*, August 2001.
- [13] Edward G. Amoroso, *Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, Traps, and Response* (San Francisco: Intrusion.Net Books, 1999).
- [14] Rebecca Bace, *Intrusion Detection (Technology Series)* (Toronto: Macmillan Technical Publishing, 2000).
- [15] Rik Farrow, *The Strengths and Failings of Intrusion Detection Systems*, Network Defense Column for *Network Magazine*, July 1999.
- [16] Susan C. Thomson, *Schools worry about music Web sites jamming networks*, *St. Louis Post-Dispatch*, The Detroit News, 17 February 2000, <<http://detnews.com/2000/technology/0002/20/02180009.htm>>, accessed 15 April 2004.
- [17] Ellen Messmer, *Jamming, Military Style*, *Network World*, July 2001, <[http://www.nwfusion.com/archive/2001/122072\\_07-02-2001.html](http://www.nwfusion.com/archive/2001/122072_07-02-2001.html)>, accessed 15 April 2004.

## NOTES

1. These systems include power distribution grids, air traffic control, telecommunications networks, and so on.
2. This does not diminish the need to also examine important issues in computer network security from a civil and criminal point-of-view.
3. For consistency with other doctrines, the term 'computer network spectrum' is used to denote the controllable space of computer networks and includes, but is not limited to, such things as network domains, network addresses, physical infrastructure, and all contained information.
4. For the purposes of this article, the radar band systems are considered representative of other spectrum components (communications, infrared, millimetre wave, and so on.)
5. More than a cursory comparison of CNA to EA is not possible without access to the classified doctrine of CAN.
6. "EW reprogramming is the deliberate alteration or modification of EW or target sensing systems in response to validated changes in equipment, tactics, or the EM environment [5]." Similarly, CN reprogramming would likewise be the deliberate alteration or modification of its systems to meet changes in its equipment, tactics or environment; for example, firewall rule updates.
7. In CN terms, direction finding expands to include various aspects of network topologies as opposed to just traditional geographic coordinates.
8. A 'honey pot' is a computer system set up on a network for the purpose of attracting and observing attackers. The honey pot has no real legitimate users, but it is instrumented to allow observation of attackers. A network of honey pots set up to look like a workgroup is a 'honeynet.'
9. Just as EW frequency deconfliction supports continued use of the EM spectrum in the presence of both friendly and enemy EW activities, CNW network deconfliction allows for continued use of the network spectrum in the presence of friendly and enemy CNW activities. Example systems include IFF (EW) and VPN (CNW).
10. The term 'system' is used here quite loosely when referring to CNW, as many support tools are not yet fully developed or incorporated into full systems.
11. Note that a warning does not have to mean that an individual is involved and can include warnings to other systems, such as a gateway.
12. The term 'network jamming' already exists in several usages, ranging from something close to the intended meaning in this article [16], but in a very limited and unintentional sense, to a more traditional connotation of jamming as applied to wireless networks [17]. The former is not nearly broad enough, while the latter is really just an application of traditional EW.
13. Essentially there are no known ones.
14. In the context of this scenario, the attacker is considered the red team (enemy) and the defender the blue team (friendly).
15. Imagine that the conventional attack example is an air force one.
16. A port is the communication end point on a computer, like a numbered mailbox. Each network service, such as mail, chat, HTTP, and so on, uses a different port.
17. A virtual weapon might include things such as viruses, worms, Trojans, backdoors, root kits, and so on.
18. For lack of a defined term, the installation phase of a computer attack refers to the sequence of events wherein the attacker 'installs' onto one's network a payload intended to facilitate attack (compromise). An example might be the installation of a 'Trojan' or 'backdoor.'
19. In a Denial of Service (DOS) attack, an attacking computer sends network packets to a target computer. The packets are either deliberately constructed to exploit some known vulnerability or bug in the target that will cause it to fail, or the target is flooded with packets and legitimate communications are disrupted. A Distributed DOS attack (DDOS) is launched by several attacking computers against the target. CNJ techniques are further described in Table 2.
20. Lethal in this sense implies that the victim node is taken over or compromised.
21. Again, all CNJ techniques are described in Table 2.