The 11th ICCRTS
Coalition Command and Control in the Networked Era

#1-047

Cambridge, England
26-28 September 2006

Draft

Paper Title

Network Centric Principles and World Cargo Security

Topics
Network Centric Metrics
Lessons Learned
Coalition Interoperability

Authors

Barbara Torell
Chair: Business Management
Leibniz Open University -Milan
Mail address:
Via XXVII Maggio, 46
22100 Como, Italy
Tel: +39 031 576 191
Fax: +39 031 338 0165
Email: batorell@tin.it

Salvatore Fiorillo
Information Security Consultant
Theosecurity
Via Borsieri, 11
20159 Milan, Italy
Mobile: +39 3381061725
Email: sfiorillo@theosecurity.com

Abstract

The focus of this paper's scrutiny is on maritime transport security measures for cargo supply chains. A primary objective is to identify potential vulnerabilities in the general context of threats and determine which risks should be considered. Since seaports maintain a critical role in the transit movement of water-borne cargo and commerce, a major effort has been directed toward enhancing the security of container shipments. In response to the 9/11 terrorist attack, U.S. agencies instituted a series of initiatives that address various points of vulnerability.

The goal of borderless security is addressed with a recommendation that offers a Network of Shared Awareness [situational]. Crucial to the network are Complex Adaptive Systems [CAS], which are dynamic entities able to adapt instantaneously to radically changing environments. The aim of the paper is to explore innovative ways that anticipate and react to disruptions in the global cargo supply chain. The results of the research indicate that current weaknesses in cargo security can be improved.

Firstly, traditional methods have been found lacking when confronted with terrorist tactics including undue advantages [Flags of Convenience, Laws of the Sea]. Among recommendations, ***learning from the enemy*** *is paramount, especially in a new defense environment. Complex Adaptive Systems [CAS] provides a coherent starting point for moving from the uncertainty of threats to acceptable risks. This paper recommends the use of Complex Adaptive Systems [CAS] to counteract the imposed limitations of the International Law of the Sea. The primary dilemma: International law denies the boarding of sovereign-flagged vessels on the high seas, including vessels with FOC [Flags of Convenience].*

.

We argue that should the cargo industry be manipulated to a point of vulnerability, a terrorist attack would probably prove successful. This assumption turns on the fact that current practice hampers traditional methods of defense-that are in fact out-of-date. Secondly, legal restrictions deter investigative practices such as boarding and searching a suspicious vessel for dangerous cargo contents. One pivotal but controversial issue is discussed: the registering and flying of flags of convenience. While National security coalitions, including coast guard units, have agreed to comply with the Law of the Sea, signers of the Proliferation Security Initiative [PSI] may not. As an alternative, this paper suggests ways to respect the Law without taking unacceptable risks with national security.

.

Key terms:

Coalition interoperability, network centric, complexity, sense-making, shared awareness, adaptive, uncertainty, interconnectivity, risk

Introduction

Clearly, the September 11, 2001 terrorist attack on New York changed the world and the consequences for globalization. The interactivity and connectivity of the global market was altered and a new reality introduced. Moreover, the security crackdown that followed has affected every facet of the global economy. Indeed, globalization itself has transformed the way security is managed in much the way it has changed economies. Two weeks after the attacks, Stephen Roach (2001) the chief economist at Morgan Stanley declared that "Terrorism puts sand in the gears of cross-border connectivity and the result threatens the increasingly frictionless world of globalization."

In fact, globalization not only reformulated the economic competition [and policies] within countries, it also influenced the character of actors and institutions within world politics. What's more, in a global governmental system created for 51 countries, 193 states now partake of a sovereignty which is becoming more diffuse. Regularly, new 'stateless' multinationals (e.g. Chiapas and Chechnya rebels, Tamil Tigers etc.) arrive 'on a world stage that is essentially 'borderless'. Moreover, thanks to the global media, rebels and terrorists currently "enjoy a greater capacity to publicize themselves and gain an audience" (Woods 2004:467):

> These new actors cut across the traditional structures of state sovereignty and inter-state order, challenging governments and demanding access to the inter-state organizations charged with global governance. Indeed, the very principles on which sovereignty is recognized and respected are changing, so that, in words of an international law scholar, we are faced with an 'impossibility of reconciling the notions of sovereignty which prevailed even as recently as 50-60 years ago with contemporary state global interdependence.'

Transnational, non-state terrorism is the new maritime reality; one that creates a formidable dilemma by weakening our response capability; especially when rogue actors use a variety of means (e.g. piracy, *Flags of convenience*)[1] to circumvent state security. Sovereign states will remain victims of private actors--in this case, terrorists—if they fail to "eliminate these groups by depriving them of sanctuaries and punishing the states that harbor them" (Hoffmann 2004:107). Not surprisingly, as Hoffman emphases, national interest of an abused state will demand either "armed intervention against governments supporting terrorist or…prudent and discreet pressure on other governments to bring [them] to justice". In the end, the current era of "a war on terrorism" has no sovereign enemy target. Neither insurgencies nor terrorists represent conventional adversaries in traditional military operations. What we are dealing with, insofar as terrorism is concerned, is not war but unfulfilled threats. Although the threats were made real on September 11, 2001; since then, no other threat has been actualized on US soil; albeit, others, horrific ones, were achieved in Madrid, London, Bali, Egyptian resorts, and elsewhere.

Nonetheless, non-actualized threats directed to both the US and foreign maritime industries did heighten after 9/11 and an aggressive response is ongoing, mostly directed to the vulnerabilities of water transport. Security problems, initiated by the maritime container trade, point to non-state actors and especially to their open access to all forms of communication. Unlike previous modern

[1] Discussed on page 7

devises (e.g. fixed-line telephones, computers, television, radio, etc.) requiring infrastructures that separated rich nations from poor nations, current networking technology is openly available to anyone: friend or foe. In addition, an overriding concern is the smuggling of WDM (i.e. weapons of mass destruction) somewhere amongst the 7 million ocean containers that arrive annually at US seaports (GAO 2003). In sum, the rules have changed or no longer exist; instead a new dynamic environment has emerged, connecting nodes, people and markets.

What kind of new dynamic environment are we talking about? In this case, an environmental network that is symbolically ‘flat’. Indeed, Thomas Friedman’s (2005) last book describes this global entity as a *flat world;* albeit one with complex networks integrating all facets of our existence—most especially through the interactivity of markets. For instance, globalization connects the Chinese textile shipper as well as the Afghan opium poppy grower exporting crops to first world markets (Atkinson & Moffat 2005).

Cargo security is a serious issue, but not the only one. Indeed, security needs are found everywhere. Yet while security forces (i.e. law enforcement, military and public) are merging efforts, more speed and breadth are required. Agility and a common shared awareness are tantamount in the quick response to an actualized threat and the dissemination of information seamlessly. The breakdown of information flow during the panic of 9/11 demonstrated the vulnerability of a purportedly top tier communication system. One issue, the unregulated use of Flags of Convenience [FOC], looms large as a major contributor to maritime vulnerability. The issue is intrinsically tied to the Law of the Sea (i. e. potential for international treaty violation). The standoff arises when a security force attempts to enforce the Proliferation Security Initiative [PSI][2] when boarding a suspicious, sovereign-flagged vessel. At bottom, ‘chaos and crime’ abide on the world’s oceans and hence present security challenges that are often non-existent on land.

The paper opens with a brief overview about containerization, vulnerabilities, and current security measures [i.e. Initiatives]. Two network-centric systems are introduced (Complex Adaptive Systems [CAS] and a Shared Information Awareness [SIA]) and discussed, including the overall efficacy of network centric systems. The research study itself is both expositional and analytical in that it identifies problems and uncovers unforeseen weaknesses within the cargo security campaign.

Part One Containerized Cargo: Background of the “black box”[3]

If not for Malcolm McLean, the global economy probably would not exist (i.e. as we know it). In 1956, McLean, an American trucking magnate, concluded that ports were disorganized and chaotic places and impossible to calculate the time involved for shipping goods from one port to another. He proposed and delivered a standardized container that increased the logistics of efficiency and prevented thievery. However, a standardized container required new vessel-types and specialized trucks to haul cargo containers to and from port terminals—without ever using human energy to move goods. Today, global commerce relies on *Intermodal shipping containers* transporting almost 20 million containers worldwide; yet, the industry would not have grown as rapidly without McLean’s interest in ‘logistics’. Ironically, McLean ushered in a modern industry that only caught on during the Vietnam War when speedy deliveries of war *materiel* to US forces were essential

[2] See initiatives page 6

[3] The “black box” is a metaphor representing the lack of visual access to the contents of the cargo container and by extension, its ‘anonymity’

(Caryl 2006). Overall, the cargo transport industry's growth rate has quintupled in less than 20 years.

Safe cargo transportation entails infrastructures that physically link markets separated by vast distances. Sixty per cent by value of total world goods trade is carried by sea and 90 per cent of that goes by standardized container (Flynn 2006). At the onset after 9/11, the cargo transportation industry felt that an economic *Armageddon* had arrived; yet surprisingly fears of costly delays [including the cost of extra security measures] were found to be misplaced. Indeed, after a brief time of adjustment, shipping delays, between the larger trading partners, were reduced to 'about half a day at most' (Djankov 2006). Nonetheless, any disruption (e.g. 72-hour shut down of the Strait of Malacca) in the container supply chain caused by a terrorist incident would seriously damage merchant shipping and the free flow of goods. In short, calculated losses would result in billions of revenue.

Part Two: The Security of Maritime Trade

The logistics are both simple and complex. Research often relies more on behavior psychology than academic rigor. The fact that the "black boxes" [cargo containers] are opaque, projects an impression that the contents are totally anonymous. For instance, the anonymity of *containership* delivers opportunities for stolen cars to be hidden under stacked rows of Soccer T-shirt cartons or forbidden nuclear missiles to be buried under tons of potatoes. Of course, sophisticated screening devises exist and are used in a number of modern, up-to-date ports. Unfortunately, not all US and foreign ports are modern and up-to-date. Furthermore, a full security screening (100%) would require expensive time-consuming inspections (US screening currently at 5%) and if initiated, the smooth functioning of a dynamic supply system would be compromised (Caryl 2006). Overall X-Ray scanning cannot obliterate the lack of visual capability; the "black box" will retain its anonymity- at least for now.

Initiatives

After the responsibility of securing global trade was acknowledged, safeguards (i.e. initiatives) were put in place to prevent terrorists from using cargo containers for any destructive act. Most were coalition-type initiatives whereby international agencies and groups agreed to share information and methodology to guarantee the safe movement of trade and goods.

[1] Container Security Initiative [CSI] 2001

Only one month after the Twin Towers disaster, an initiative was launched requiring ocean carriers to provide appropriate cargo descriptions.[4] A cooperating government then forwards a detailed document of the ship's container cargo before the transport leaves the foreign port. At the receiving end, the US Coast Guard analyzes the security risk based upon what is known about the shipper [including history of the container] and makes a decision as to whether it should be X-rayed, screened by other detectors, and/or opened and inspected. As mentioned earlier, only 5 per cent of incoming cargo to North America is currently screened. When considering a cost-benefit analysis, there is currently no suitable method that adequately delivers 100 per cent screened, inspected containers --prior or after entering US ports. In sum, sustaining a balance between moving people

[4] A document detailing content and valid consignee addresses twenty-four hours before a US-bound cargo is loaded at a foreign port (USEU 2006).

and cargo –efficiently and safely—"without sacrificing security and privacy"—is hardly doable at this juncture.

[2] Megaports Initiative [MPI] 2003

NNSA's 2003 (National Nuclear Security Administration] Megaports Initiative, collaborates with other countries to screen cargo at major global seaports. The Initiative provides radiation detection equipment and trains their personnel to specifically check for nuclear or radioactive materials. In return, data from detections and seizures of nuclear and radioactive material are shared with all collaborating countries.

[3] The Proliferation Security Initiative [PSI] 2003: Suspected weapons of mass destruction

The Proliferation Security Initiative [PSI], the third organizing measure related to cargo transportation, includes an international coalition of sovereign states. In accordance with national legal authorities including relevant international laws (and frameworks), a collective effort among participating countries—--collaborate to prevent the proliferation [or threats] of WMD: weapons, missiles or related materials. The PSI is both observed and administered by a "core group" of nations (currently numbering 16). In some respects, security initiates, especially those originating in the US, have a history of occurring after the fact. The following narration of an actual event occurred in 2002 and became the impetus for the Proliferation Security Initiative [PSI]:

<u>Narration--Incident</u>

> *Anonymity and Free-Passage on the High Seas*
>
> Monday, December 9, 2002, approximately 600 miles off the Yemeni coast in International waters; two Spanish Navy ships were tracking the freighter *So San,* a Cambodian registered freighter [sailing without a flag] that had left the North Korean port of Nampo in mid-November. After ignoring warning shots from the Spanish ships, it was boarded and searched by Special Forces. Evidence concluded that the ships name and identification number was painted over and that the crew was Korean and not Cambodian. The captain argued that the freighter was loaded with 2000 pounds of cement destined for Yemen [verified on the ship's manifest]. Not surprisingly, the search revealed large containers of missile parts, including containers of unknown chemicals. U.S. Weapons experts were called in to verify the load: 15 mid-range SCUD missiles, 15 conventional warheads and 85 drums of inhibited red fuming nitric acid-a chemical used as an oxidizer in SCUD missile fuel. (Joyner 2004:1)

[a.] Yemeni Outcome: Avoiding an international incident

The Yemeni government confirmed that the order for the missile parts (originally authorized in 1999) was needed to upgrade the small number of SCUD missiles in their arsenal. They denied any intent to conceal the shipment, placing responsibility of the deceptive storage ploy (under cement bags) on the shipper--North Korea. After receiving assurance from the Yemeni government, the U.S. government and President Bush "signed off" on the incident, releasing the ship and its cargo*. In the eyes of existing law* – it was simply a sale of goods from one state to another (Joyner 2004). In fact, the Spanish and American ships forced the inspection and could be cited for crossing a legal line: *the right of free passage through international waters.* The President's decision to sign off was made on the following points:

1. The ship was on international water
2. It was a sale that was out in the open and consistent with International law.

Fundamentally, it is a critical initiative since it might “alter the transnational framework for the use of force by states” (Shulman 2006:3). Moreover, as Schulman acknowledges, there are statements left unclear such as designating who will be the final decision makers. At bottom, most PSI objectors seriously challenge potential legal infractions of the *International Law of the Sea* (Chaffee 2003, Joyner 2004).

[b.] “*Anticipatory Self-Defense”* [ASD]—A feasible security measure or an unworkable principle?

Although traffic in unlawful nuclear material is hardly a new game, the players are new—or at least the new ones may have been on the bench in the past. The *game rules* have decidedly changed and any attempt to adapt international laws to an unfriendly global *playing field* has spawned controversial disputes. One controversial dispute introduced by a few states concerns the previously discussed Proliferation Security Initiative [PSI]. Objections, in particular from China and Russia, mostly center on the notion of *Anticipatory Self-Defense.* In short, the opponents' objections are based on legal infractions of *The International Law of the Sea.*

> Anticipatory self-defense is defined as an attack upon another state that actively threatens violence and has the capacity to carry out the threat, but which has not yet materialized/actualized that threat through force (Joyner 2002:3)

Anticipatory Self-Defense [ASD] is hindered by at “least two limiting principles—necessity (or immediacy) and proportionality” (or comparative ratio) (Joyner 2004:3). It is clearly useful in cases of piracy; especially on the high seas, when rogue groups manipulate agreed upon measures of encounter. Although the initiative [PSI] has taken on the rubric---*‘preventive self-defense’* (by critics), the security measure [ASD] specifically references a particular cargo vessel ‘under the jurisdiction and flag of another state”, which in this case renders the initiative less useful (Joyner 2002:4). In any case, a review of relevant issues of the International Law of the Sea [LOS] might be useful given that it is probably the most comprehensive “and well-established bodies of international regulatory norms in existence” (Chaffee 2003). Furthermore, formal legal agreements are tantamount to securing a peaceful international environment. The principle points are listed below:

The Law of the Sea [LOS] grants several freedoms

1. Right to navigation on the high seas :*Rights to transit through:*
    1. International straits
    2. Exclusive economic zones (EEZ)
    3. Territorial and archipelagic waters of another state
2. A select number of illegal activities are barred: *Grants intervention in the following activities:*
    1. piracy
    2. slave trade
    3. illicit traffic in narcotics drugs or psychotic substances
    4. unauthorized broadcasting
3. The LOS does not explicitly prohibit transit of weapons of mass destruction [WMD] or gives states rights to interdict such transit.[5]
4. States of Concern (to the United States):
    i. North Korea, China, Pakistan and Iran[6]

[5] A number of states, including the United States, have actively opposed the development of such prohibitive norms or interpretations of international law that would inhibit the transit of weapons of mass destruction by the seas or air and cites the rights and privileges established under the Law of the Sea to affirm unhindered military use of the oceans (Chaffee 2003).

All interdictions, outside those explicitly allowed [i.e. WDM] in the existing International Law of the Sea regime, would be clearly viewed as violating the *freedom of navigation on the high seas and the right of innocent passage through territorial waters.* Some groups (Chafee 2003:3) favor a resolution that would support the interdiction of arms "when appropriate"; or prohibit what is deemed a threat to security; in other words, prohibit such transit as being "non-innocent". Nonetheless, the transporting of illegal nuclear material to be sold or given to rogue states remains uppermost on national agendas; especially that of the United States. Unfortunately, security interdiction policies may fail due to legal infractions. In particular, an initiative such as PSI (Proliferation Security Initiative) may be limited in its enforcement.

Part Three: Lessons Learned

a. The Pariah of Borderless Security*: "Flags of Convenience"* [FOC]

It is because national security is weakened once the transport leaves protected water that the maritime industry has maintained some form of extended *borderless security*. Furthermore, the ambiguity of a '*Borderless security*' stems from the fact that no guaranteed safe passage covers the interval between the time a vessel enters international water and when it re-enters secure water. At present, most all cargo security is dealt with in two locations: a) place of departure and b) place of entry. Notwithstanding, it is the body of water in between the two locations that is next to impossible to monitor. Essentially, the open sea offers a free zone where any [state or non-state] vessel is at liberty to move often and without detection. Moreover, the complexity of navigating an unmonitored sea is compounded by the widespread proliferation of *Flags of Convenience* [FOC].

Forty thousand ships travel the ocean, often crewed by non-union personnel, owned by off-shore "shell" companies and flying the ever-present *flags of convenience* [FOC]. Flags of Convenience [FOC] registration fees, minimal or no taxes and freedom to employ cheap labor are strong motivating incentives in a company's decision to *'flag out'* (Global Policy Forum 2005). Yet, the question: 'How does an entire ship disappear at sea; especially in the technological 21st century?' is hardly difficult, given the multitude of chimera-like methods available to potential enemies such as changing a vessel's name, sovereign flag and/or paint-job. Furthermore, during state control inspections, deficiency reporting and detentions, port authorities can choose to overlook or bypass transgressing ships flying *Flags of Convenience*. For instance, international drug cartels have long-established sea routes for their FOC registered fleet that afford opportunities for off-loading in small ports or mid-Atlantic ship-to-ship transfers.

Whether organized crime or terrorism, the ability to disappear and reappear is far less plausible on land than on sea, where a particular route taken is not immediately traceable. Since under international law, every ship must sail with the flag of a sovereign state, *Flags of Convenience* [FOC] will not disappear any time soon. In fact, FOCs pattern the long-entrenched operations of off-shore companies allowing ship-owners the opportunity to register in countries that offer tax breaks with few regulatory laws or rules. Along with the shady ownership of ships, foreign flag registrations, and unskilled, low-paid, multinational crews, controlling safety conditions or cargo

[6] All are not members of arms interdiction, thus not bound by the controls [i.e. the arms interdiction PSI]. It might be legal to interdict shipments on the High Seas that have been deemed by the Security Council or the LOS tribunal to violate the Law of the Sea and to constitute a threat to the peace.

content is next to impossible. The lack of strict regulatory control circumvents the often outstanding maritime security efforts of government and private maritime security groups. Nonetheless, the lessons learned from 9/11 are well documented. For instance, prior to 2001, Al Qaeda was purported to own (or lease) a maritime fleet estimated from 20 to 80 ships (Global Policy Forum 2005).

Above all, non-state actors are major beneficiaries in the use of *Flags of Convenience*. The quote below foreshadows the enormity of the problem:

> Due to the lack of transparency inherent in the Flag of Convenience system, it is impossible to trace them. The Tamil Tigers had a fleet of 11 commercial ships, under Panama, Liberian, and Honduran flags. Other flags have been more recently named in connection with people smuggling, drugs, and arms smuggling—notably Cambodia and Tonga. Ahmad Yahya, of the Cambodian Ministry of Public Works and Transport, is reported to have said:
>
> > *"We don't know or care who owns the ship or whether they're doing 'white' or 'black' business…it is not our concern"* (Fairplay, 12 Oct. 2000)

Indeed, all agencies involved [i.e. international, national and civil] agree that *Flags of Convenience* provide more options for anonymity. Furthermore, it's not only the anonymous transportation of drugs and illegal immigrants but also the movement of explosives and guns to terrorist operatives that concern public agencies.

b. Convergence: piracy, terrorism, and organized crime

No matter what the historical period, the physical realities of the open sea are undeniable. Indeed, 'For centuries, crime organizations have functioned seamlessly on the high seas; especially when piracy is inserted into the mix (Langewiesche 2004). Further, given the proliferation of "un-governed" marine water and FOC registered vessels trafficking in unlawful material that move along major international transport routes (e.g. Strait of Malacca), the plausibility of arriving at a workable strategy to compete with an increasingly efficient networking enemy is questionable at best. Besides the "outlaw" sea presents a new level of strategic choices; in particular, unlike other non-military industries, maritime breaches are fuelled by non-state actors.

Modern pirates are known to traffic in everything from commercial goods to unlawful nuclear materials, which may be motivated more by politics or ideology than financial rewards. What has emerged is the *maritime terrorist*, a composite of pirate, criminal and *terrorist,* united in an ideological (sometimes political) agenda. The increase in piracy, especially in Southeast Asia, is often due to a combination of several items: weak, complicit and/or corrupt states providing havens for all forms of syndicates: organized crime, pirates, and terrorists.

A convoluted group of actors [national, economic, criminal etc.] often masks the complexity of maintaining cargo security. Consider the following event: the *Winner*, a 32-year- old 5,000 ton merchant ship flying the Cambodian flag, was carrying cocaine with a street value of $230 million. Official reports stated that it was carrying a cargo of iron bound for Bilbao in Spain. The crew [mostly Greek and Spanish] and Master were linked to a Greek company headed by Anastasio Kakasidis "who is believed to have been present when the drugs from Columbia were loaded in the mid-Atlantic". By lucky chance, a French naval vessel intercepted the transport and it was relieved of its contraband after shots were fired across its bow several times. Cambodia, a sovereign state, was allowed to set up a registry in 1994 as a faster, cheaper[7] alternative to other FOC registries. Ironically, Cambodia's registry headquarters is based in Singapore; reportedly co-owned by the Cambodian royal family and a North Korean diplomat.

The most dangerous group using the ocean seas to transport illegal goods is the terrorist organization LTTE [Liberation Tigers of Tamil Eelam], a domestic group fighting to create a mono-ethnic Tamil state. It is a highly structured terrorist group that helped train the original Al Qaeda organization. The LTTE terrorist network, spanning almost 50 countries, trains recruits, operates highly technological equipment as well as finances, and runs shipping groups. Indeed, the LTTE is one of the few terrorist groups with a state of the art shipping network.

Since 1995, Al Qaeda has made use of LTTE transports to move weapons and trainees to distant operation locations. Indeed, the LTTE-Al Qaeda alliance has been instrumental in improving Al Qaeda's information technology equipment (e.g. access to V-Sat equipment) and tactics, especially its land and sea technologies [e.g. the *USS Cole* attack in Yemen-2000). The following excerpt from September 2001 describes the operation (Ahmed 2001 September 22):

> As Asian intelligence agencies have learnt one LTTE combat trainer and an explosives expert helped train Al Qaeda men in Afghanistan. The linkages throw up disturbing possibilities. Gunatna warns that 'governments just won't have the lead time if terrorist groups cooperate like governments to share intelligence and even sometimes transfer funds, because whatever terrorist technology is available in one country will soon be available in another.' Intelligence sources said that the Islamic-secular model of cooperation between the LTTE and Al Qaeda was subsequently reflected in the tactical alliance of similar outfits in South-East Asia.

A major US interest, especially in terms of port security, relates to whether terrorists might use a ship carrying explosives to blow up a major port, or distribute arms to terrorist cells within a community. A more plausible scenario might pattern the 1998 bombing of US embassies in Kenya and Tanzania. The bombings are well-documented maritime cases of al-Qaeda terrorist successes due to the fact that explosives were received from a rogue, *Flag of Convenience* off-shore vessel (*Times India* 2000). Other maritime scenarios include one from scholars Luft and Korin (2004) who predict a massive economic energy [oil/gas] disaster brought about by a blockade of the Indonesian triangle; in particular, the Strait of Malacca. In sum, any guarantee involving maritime security remains mostly absent due to the complex networks (i.e. state, non-state, and/or unlawful groups) operating on the high seas under *Flags of Convenience.*

Part Five: Collaborative Environment: Building a Global Information Awareness Network

As a result of researching this document, we have entertained the notion that cargo security is very much like internet security. For in both fields there is a sender and a receiver, including awareness that no one trusts anyone else. However, in network security the burden to verify the payload of a TCP packet or session is up to the receiver; whereas in cargo security there is a tendency to solve the problem at its origin. Moreover, similarities in both models exist, if only from a security-deceptive point of view. In defending a network, it's possible to deceive attackers by putting in place first-class firewalls, Intrusion Detection and Prevention Systems (IDS and IPS), Antivirus or

[7] Some FOC registries can run in the thousands with flags arriving by postal service

even Honey-pots[8] and Honey-nets. Also many initiatives, such as those previously mentioned, are functioning; yet in both cases, security means nothing if there is a secondary door where attackers can enter. In the network case, the secondary "door" could be an unauthorized modem (used only to dup proxy restrictions). In the maritime case, it could be a second-class port where no one bothers to inspect or protect (not to overlook the fact that only about 5% of the cargo is regularly scrutinized in first class-ports).

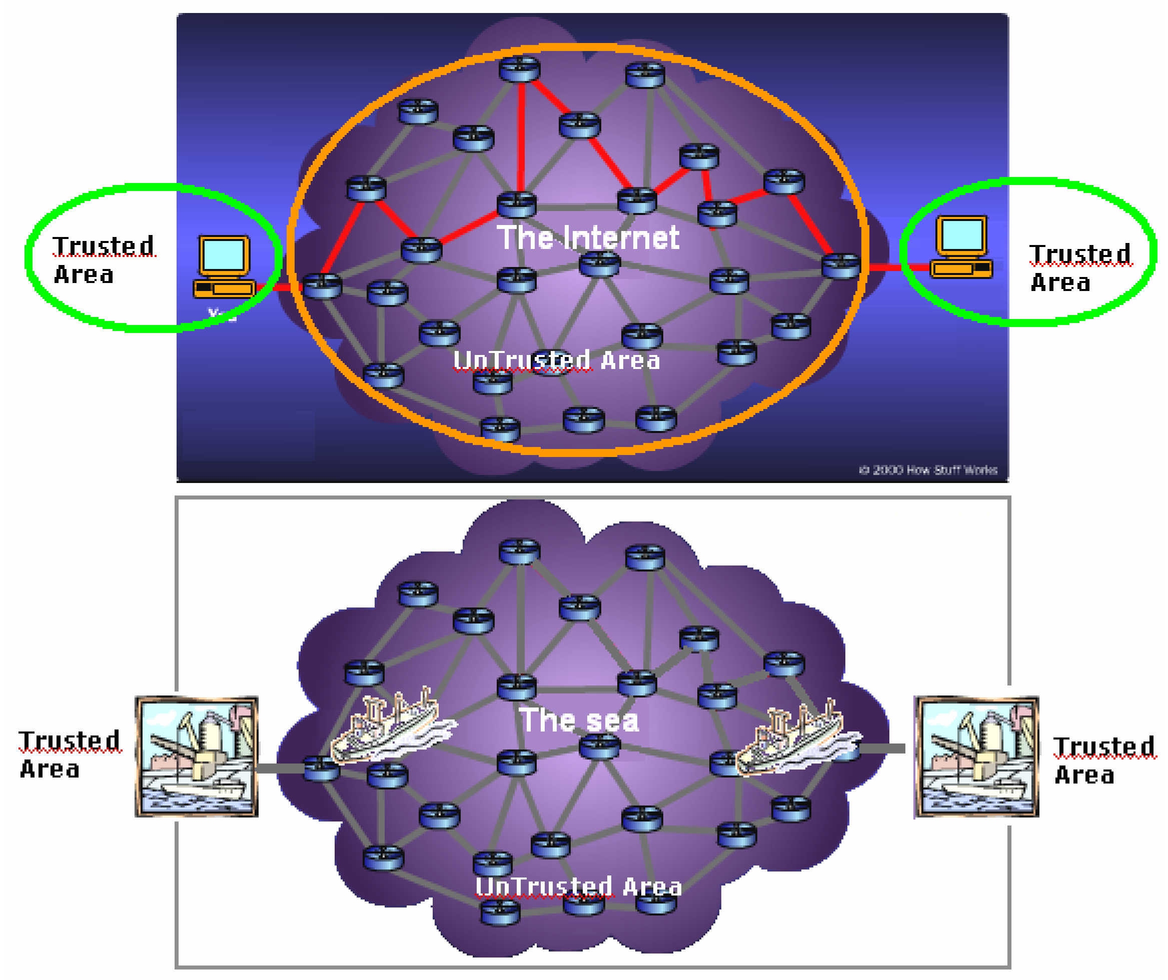


Figure 1. Network Security and Cargo Security could share same issues on trust

As might be expected, there are other similarities in network and port security such as **de-fragmentation** (reconstructing innocuous, fragmented payloads at destinations to build a lethal payload, such as a multi-part bomb set to trigger once all components are in the same area), **packet flooding** (flooding a high security port with inoffensive containers could have led to its unavailability and thus lead to its substitution with another less-protected one), **covert channel** (a combination of colors and logos on containers could be used to send scrambled information in a

[8] Honey-pots are a fake, only virtual, computer exploited by attackers yet containing un-useful information. It's a way of inducing an attacker to waste time and while we study his behavior.

very open field), or **man-in-the-middle attacks** (that is, the possibility to change container content – in high seas- without noticing sender and receiver).[9]

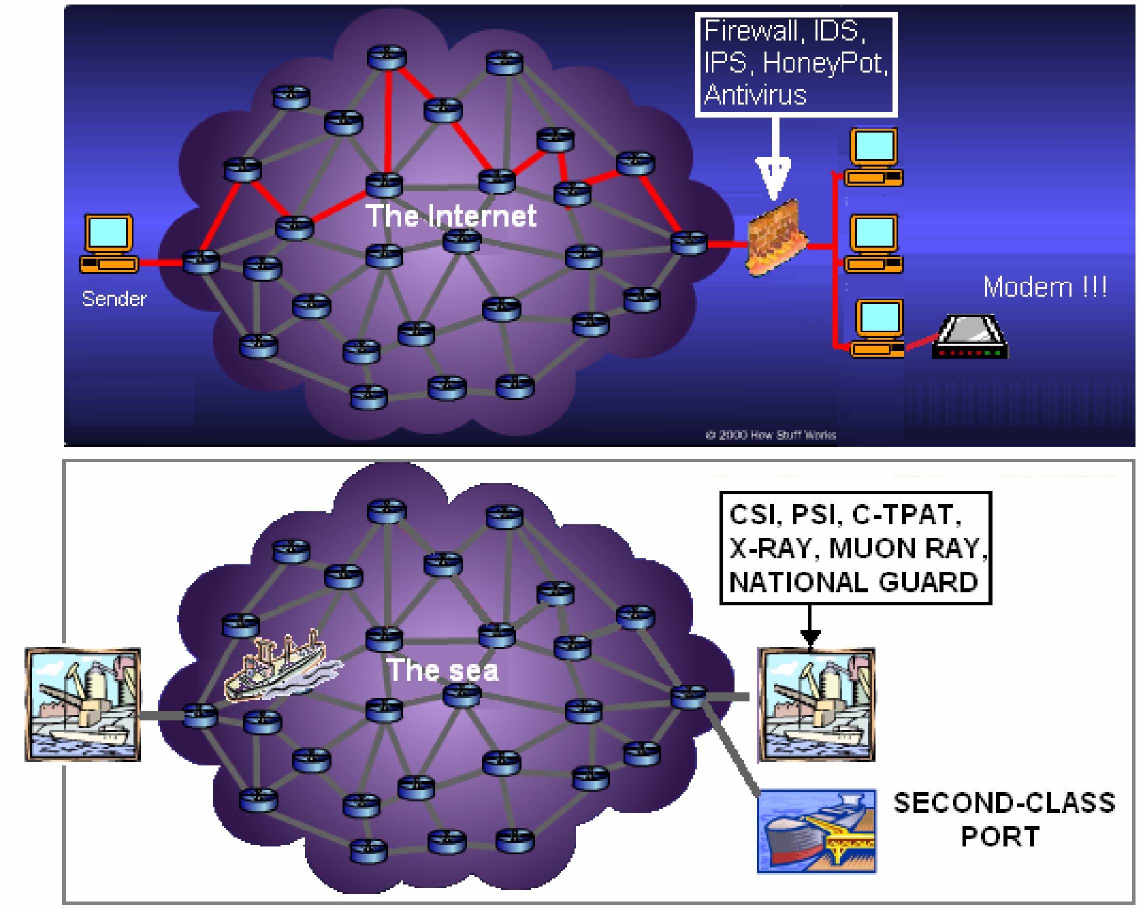

Firewall, IDS, IPS, HoneyPot, Antivirus
The Internet
Sender
Modem !!!
© 2000 How Stuff Works
CSI, PSI, C-TPAT, X-RAY, MUON RAY, NATIONAL GUARD
The sea
SECOND-CLASS PORT

Figure 2. Security is a chain and the weakest ring is its strengthens

Increasingly, even virtual relationships between terrorist networks and criminal organizations could lead to new asymmetrical challenges (Prefontaine and Dandurand 2004). If this prognosis proves accurate, a global civil-military coalition will require a collaborative environment, one that delivers seamless, integrated communication. In addition, what should emerge is a shared-situational awareness amongst international groups; specifically, one comprised of both military and law enforcement. Nonetheless, this is an aggregated problem since networks suffer some form of entropy [“the complexity of warfare”[10]] that is unavoidable. In these cases, while the trust required would guarantee the sharing of information, it would hardly be achieved by *contract.* The next section examines this issue.

[9] Useful (and even humorous) reading on this topic: *Secrets and Lies—Digital security in a networked world* (Schneier 2000)

[10] ‘The seeming randomness of warfare is really the interaction of many influences’

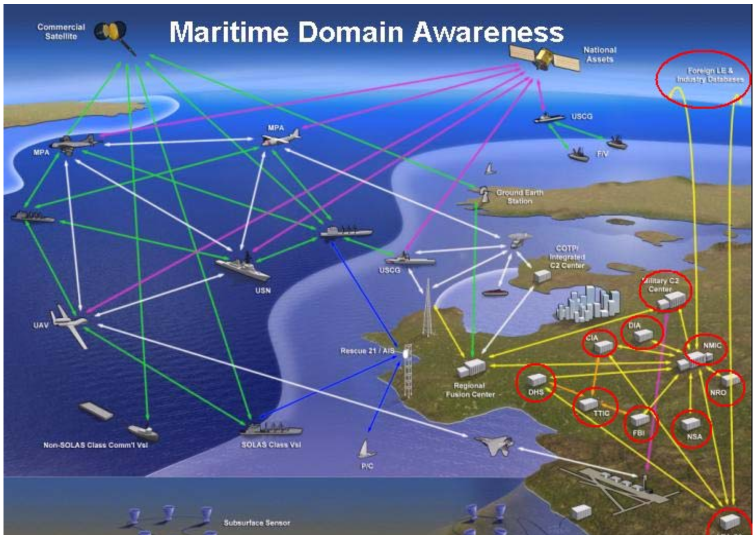
1. Shared Information Awareness Network: *How much uncertainty should we accept?*

Sharing information [i.e. a form of trust] can be 'counter-cultural' to most individuals and organizations involved in military or Intelligence agencies. Nonetheless, trust is a prerequisite for information sharing. However creating trust in a networked environment is hardly easy; especially when individuals have not worked together nor developed a common bond. While less than ideal yet often necessary, individual contact is all but exclusively electronic-generated. On the other hand, uncertainty is inescapable when trust is less than assured and security is less likely. At bottom, individuals, often with good intentions yet unaccustomed to working together, might experience difficulty when making sense of information they have not directly gathered.

The "Mann-Gulch" disaster (Weick 1995) remains a good example for demonstrating what people (not used to physically working together) might think is best to do under pressure. On the other hand, while networks are the best means for sharing data, they may not be a valid tool for sharing knowledge. For instance, the Challenger disaster (1986) might have been avoided if decision makers had read the body language and subtle spatial behaviors that were transmitted during the videoconference between a key NASA contractor, Morton Thiokol and NASA's project manager (Boisot 2002).

2. The U.S. Maritime Domain Awareness (MDA) program[11]

The *Maritime Domain Awareness* [MDA] is "the effective understanding of anything associated with the global maritime environment that could impact the security, safety, economy, or environment of the United States." Its orientation is toward achieving complete maritime visibility and protecting national interests. The MDA mission is to provide decision makers at all levels with an effective understanding of the maritime environment. While the MDA is an interesting program, it is no more than a clone or a sub-representation of the Global Information Grid[12] (GIG) tailored on maritime security. Again it is a valid program to share data between electronic networks, but it seems less focused on addressing the problem by deploying a type of sense-making that is commonly accepted and understood whenever the unexpected occurs.



[11] Further information on the program can be found at MDA website www.uscg.mil/mda/

[12] For more information on GIG –http://www.nasa.gov/ia/industry/gig.cfm?MenuID=10.3.2.2

3. Complex Adaptive Systems[13]

In the following case, the term *complexity* refers to the theory as applied to Complex Adaptive Systems [CAS]. These are dynamic systems able to co-evolve and evolve within, or as part of, a changing environment. It is important to note, however, that no dichotomy exists between a system and its environment, in the sense that a system always adapts to a changing environment. Rather, the notion to be explored is one of a system that is closely linked with all other related systems that make up an "ecosystem". Within this context, change needs to be seen in terms of co-evolving with other related systems, rather than as adaptive to a separate and distinct environment.

The following image will be used along with subsequent ones to demonstrate the use of CAS in this paper.

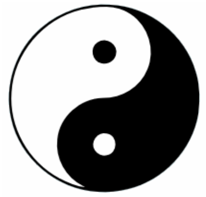


Figure 4. CAS representation

The White and Black areas represent components belonging to the same networks, organization or entity. However, the image is not a static representation of the CAS state, since it is in a fluid and relative state of balance. The White is the useful part for 'mission accomplishment'. The Black area of the component is not useful since it is only a functional part of the system or represents a system's error or limitations (some CAS systems cannot perform actions that others can). The agility of the CAS is due to its capability to balance and optimize its resources in the operating contest. The small dots represent the entropy of the system. The black dot in the white area represents the following: a system error, law limitations, insider activities (mole), the effect of Effects-Based Operations of a foe, the incompatibility of a component's background (i.e. political or religious) with the mission requirements and purpose (eliminating the enemy). The White dot in the black area could represent underestimated resources. The border separating the black field from the white is the border of attrition (to be discussed with the CAS fighting). It might be argued that 50% of the black area is not correct (too high a ratio). This might be valid, but it is difficult to define the correct ratio; nonetheless, it should be remembered that Pareto's law argues that 80% of our successes are due to 20% of our total efforts.

[13] See Atkinson and Moffat 2005 for extensive discussion.

The following image of a CAS representation might be useful for a better understanding of the kind of force a network would need to manage within itself. Putting the CAS model in the Network Centric arena with its new C2 scheme allows for an immediate understanding of *Network Awareness,* Time for '*Mission Accomplishment'*, Self-Synchronization, and all other NC components, which cannot be achieved without cost considerations. If the network consists of civil and military forces, *trust* will be a major issue as well as the absence of common sense-making. On the other hand, if the network is made up of street gangs and Transnational Criminal Organizations [TCOs], the problems would not be much different.

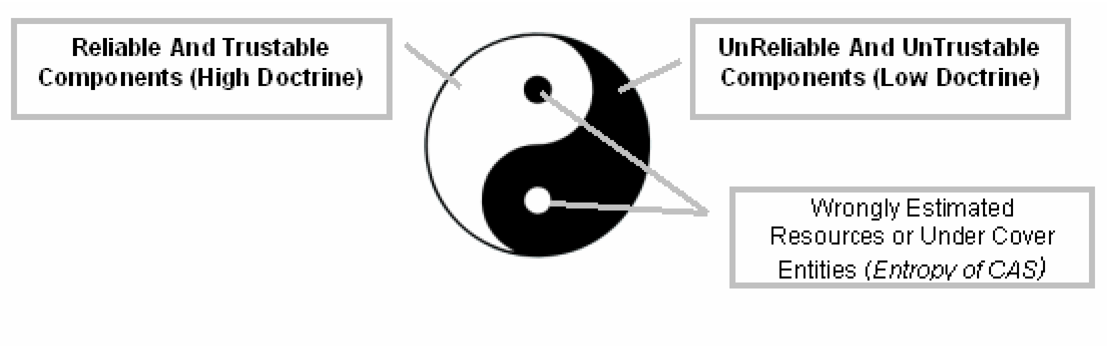

Reliable And Trustable Components (High Doctrine)
UnReliable And UnTrustable Components (Low Doctrine)
Wrongly Estimated Resources or Under Cover Entities *(Entropy of CAS)*

Figure 5. CAS components

It is a fact that the disclosure of pictures about the Abu Ghraib abuses has had an effect on the doctrine, trust and self-estimation of the West regarding the liberation of Iraqi citizens. Similarly, forcing cooperation between un-trusted networks could be an issue not only for information dissemination but also that of integrity. Both scenarios might be represented on the CAS image below as a greater black point in the white area.

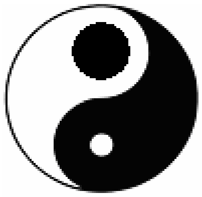


Figure 6. The representation of errors within the reliable area

4. White Hat versus Black Hat--CAS

The need for Law Enforcement Agencies to cooperate at all levels (military with civil and private forces) was discussed earlier. Black-Hat CAS and White-Hat CAS face common issues (e.g. trust, information flow inside the network and the lack of commonality of sense- making). For example, terrorists involved in the 9/11 attack on the World Trade Center were already in the United States long before that event. They were inside the nation's boundaries, training, traveling, shopping in commercial centers, using credit cards, driving cars, renting hotel rooms before they hijacked planes to use as missiles of destruction. On 9/11, terrorists exploited the entropy (or weakness) of linear thinking. In this case, the C2 model, coming from the Industrial Age, is based on *decomposition and specialization,* thus allowing for a lack of coordination between top and low Law Enforcement Agencies (e.g. Zacarias Moussaoui was already under the FBI lens), who failed to stop him)—demonstrating a lack of common sense-making between the LEAs (Law Enforcement Agencies). Solving the problem by empowering the edge is not an easy task. In sum, the improved agility of WH-CAS can be achieved by reducing its internal errors and entropy; thus leading the CAS itself to a better performance. Three major issues require individuation: the top-down approach, an information security policy-acknowledged model, and better management of human resources in the post-confrontation phase.

5. The Top-Down Approach

Many Law Enforcement Agencies [LEAs], especially non-military, call for more cooperation with other LEAs. They recommend common sense-making and improved information-sharing. Nonetheless perception continues that all proponents want to remain at the top of the decision 'chain'. That is to say, they seem willing to share information yet remain in control of final decisions. In this case, achieving collaboration or agility is highly unlikely.

Even if Boisot's paradox of information value (information hoarding and information sharing) will not be addressed in this paper, we nonetheless, suggest that WH-CAS consider deploying 'common sense-making' rather than concentrate solely on decision making capability. Still, the decision making capability must be delivered through common reach-back capabilities extended by common efforts and professionalism.

6. The need for an information security policy-acknowledged model

Another aspect includes the implementation of a multilevel-information security policy model, such as the Bell-LaPadula model (Bell and LaPadula 1976). This model reflects the way organizations access information and gather intelligence in sensitive areas. For instance, agents at an intermediate level can write to their superior (write-up) and read at a lower level. They are unable to read-up (avoiding access to unauthorized information) nor write-down (delivery is controlled).

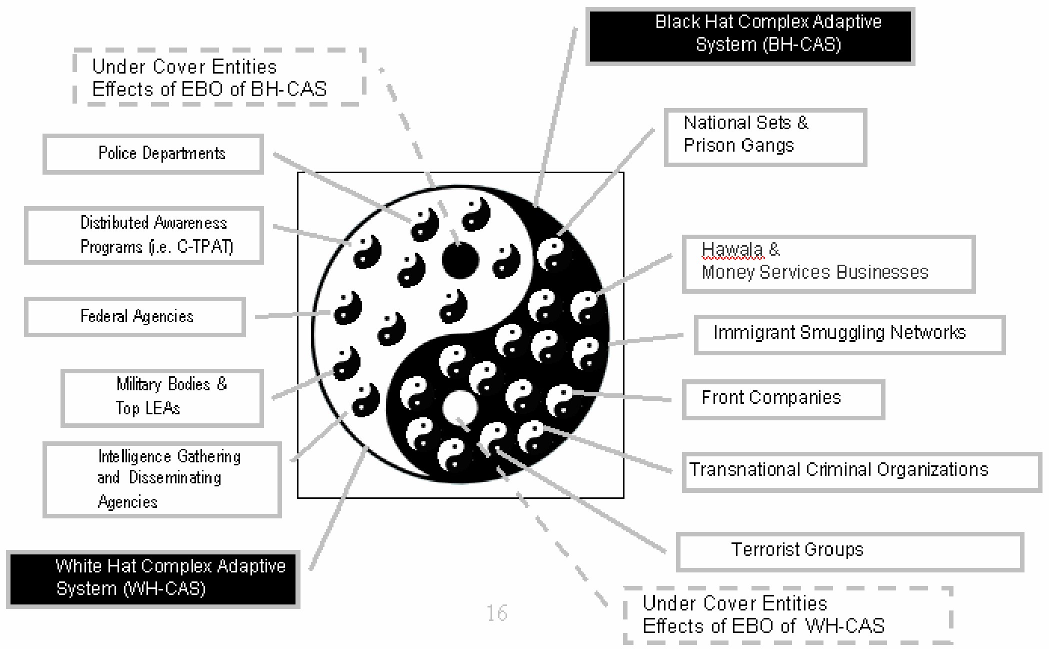

Black Hat Complex Adaptive System (BH-CAS)
Under Cover Entities Effects of EBO of BH-CAS
Police Departments
National Sets & Prison Gangs
Distributed Awareness Programs (i.e. C-TPAT)
Hawala & Money Services Businesses
Federal Agencies
Immigrant Smuggling Networks
Military Bodies & Top LEAs
Front Companies
Intelligence Gathering and Disseminating Agencies
Transnational Criminal Organizations
Terrorist Groups
White Hat Complex Adaptive System (WH-CAS)
16
Under Cover Entities Effects of EBO of WH-CAS

Figure 7. A CAS representing entities involved in the homeland security in OOTW

When adapted to a network centric group, this model would stop the flow of information, disallowing agents operating at the edge[14] to enrich their power (causing a loss of agility). The problem remains: How to balance information flowing from the network and yet deploy *common* sense-making from the *edge?* Moreover, how much information would an *'edge'* agent acquire in order to deploy one's decision-making power? All in all, the "*In God we trust*" principle, while showing the need to trust somebody, reveals a tendency to trust no one. In short, *trust* remains the discriminate for the quality of the network.

At this stage, the essence of security and homeland defense seems clear, particularly when multilevel and transactional cooperation would require immediate resolution--within friendly lines. The first requirement is to *dissipate the fog* existing between networks working on the same side. With Network Centric Organizations, we should be able to grasp some insights from computers and network security systems; for instance, within computer security there are TCSEC requirements that define a trusted computer.[15] Furthermore, in network security there are no comparable models, only policies and good practices. This is to say that network security (of machines or people) is an oxymoron. The only suggestion we offer is to strive for improvement in trust, honesty and self-respect.

> Partnerships that endure are likely to be those that adhere to Campbell's three imperatives for social life, based on a reanalysis of Asch's (1952) conformity experiment:
> (1) Respect the reports of others and be willing to base nbeliefs and actions on them (trust);
> (2) Report honestly so that others may use your observations in coming to valid beliefs (honesty); and,
> (3) Respect your own perceptions and beliefs and seek to integrate them with the reports of others without deprecating them or yourselves (self-respect)
>
> (Weick, 1993)

2. Human Resource Management in the Post-Confrontation Phase

Finally, we should stress the need for an ethic. Without a sound, sincere ethic no mission could be accomplished with acceptable satisfaction. Some years ago, one of the authors was asked to help with the merger of two companies operating in the same field. For months we tried to deploy policies, models and most of all find a solution which allowed good minds to work willingly together. It was initially an unsuccessful effort, but we later received some suggestions about playing soccer with teams made up of employees from the merged companies. The situation improved greatly during and after confrontations with other companies; for in this case, personal pride was postponed for the success of the team. Even then, a few incidents demonstrated the depth of their anger; yet they found out that teamwork was a good method for discharging built-up aggression. Oftentimes disgruntled employees, feeling less than appreciated, depict potential security risks (ComputerSecurity Institute, 2005, Mikkers, 2005). At times, the CAS model mirrors similar situations by imitating the black dot in the white area. For in the future, aspects of ethics and human resource management will most likely be confrontations involving peacekeeping operations or Operations Other Than War [OOTW}.

[14] Accessing information, expertise and the elimination of procedural constraints (Alberts/Hayes 2003:5)
[15] Now superseded by more unrestrictive, heuristic requirements that define a trusted network

Part Six: The Efficacy of Network Centric Organizations?

a. Terrorist Networks

Terrorist networks, as one of four examples of scale-free[16] social systems, sustain an efficacy that is difficult to match. As Perrow (2004:111) points out, scale-free systems avoid the perils of micromanagement by providing distribution not dominated by any 'representative scale'. For example, in a network centric system [NCW], the top tier represents the "centric" and has access to all information as needed; yet relies mostly on summaries (i.e. to avoid overloading the tier). Contrastingly, a terrorist network manages "with only highly aggregated information processed at the lower levels". Terrorists, through their networks, disseminated orders widely, mostly about their "financial flows, major targets and timing, and media activities". For all systems [e.g. network centric organizations, networks of firms, terrorist networks, and electric grids] Tier Two is spatially disaggregated (i.e. non-collective, not the sum of its parts), independent and a self-sustaining, decentralized unit.

Nonetheless, there remains a fundamental *interconnectivity*. At bottom, both enemies and opponents share a common thread of what Perrow (2004:144) calls 'radical decentralization'; in particular, the lowest level units are, in a sense, self-organizing and, "to a high degree autonomous" (i.e. free of micromanagement). Furthermore, vulnerabilities loom large on both sides: NCW requires shared complete information and should focus more on how to perform without it, while the terrorist network operates just the opposite in sharing very little. In particular, "It's (the terrorist network) reliability has to do depend upon a simpler and more expensive form of redundancy: (replacement redundancy)—if one cell is disabled, another must take its place" (Perrow 2004:116). The assessment of NCW is critical since its functionality is highly important to the overall security of the maritime community. Moreover, the military and business transformation produce an integration that is both innovative and disruptive. The two communities are together in this post-modern world and share public/private infrastructures. In sum, vulnerabilities introduced by "the interdependency, complexity, and the marriage of IT and military systems call for an evolutionary approach to NCW transformation" (Gansler and Binnendijk 2004:11).

Above all, not only are the demands for new models of security a direct result of globalization but also the interconnectivity within the maritime industry itself. While maritime trade has expanded worldwide nowhere is the increased demand more evident than in the narrow sea transport passages; particularly, chokepoints such as the Strait of Malacca, the Strait of Hormuz, and the Strait of Bosporus[17]. Indeed, past pressure on Iran over its nuclear program documented 'ominous statements' from senior Iranian government members indicating that Iran could easily block the two-mile wide channel of the Strait of Hormuz[18], and use missiles to strike tankers and …oil facilities (Belmont Club 2005).

Not surprisingly, several experts (Pelkofski 2005, Belmont Club 2005) support the premise that the next serious attack will probably arrive via a well-organized maritime campaign. As mentioned earlier, documentation of Al Qaeda's maritime capabilities was established early in 2002, with

[16] Units added without increasing hierarchy.

[17] The only connection between the Black Sea and the Mediterranean Sea.

[18] Currently about 40% of the world's crude oil shipments pass through Straits of Hormuz and the U.S. Energy Administration projects that oil traffic through the same Straits will rise to about 60% of global oil exports by 2025 (Belmont Club 2005).

classified information reporting the existence of a terrorist fleet. Although maritime terrorism is not a new phenomenon, it is one that has been active for several years, mostly in South-East Asia under the tutelage of the LTTE [Liberation Tigers of Tamil Eelam]. Further, most of the maritime training originated during Al Qaeda's collaboration with the LTTE. Some expert strategists such as Captain Pelkofski (2005:1), US Navy, strongly predict that "Al Qaeda can attack, has attacked, and will attack maritime targets". Of course, when compared to land attacks, incidents of maritime terrorism are rare. Nonetheless, recent events give pause to an impending 'overdue' unfulfilled marine threat; and thus a call for a realignment of defense against 'an expansive maritime terrorist campaign' (Pelkofski 2005).

Part Seven: Considerations and comments

In this paper, the new maritime security paradigm is reviewed and found lacking insofar as securing ports and cargo are concerned. The current debate revealed that some US port Initiatives (i.e. CSI and MPI) are less effective since vessels and cargo (both containers and bulk) are more vulnerable after leaving a port and thus, provide few guarantees that the cargo will remain tampered-free before the designated port of entry. Separately, the controversial Proliferation Security Initiative [PSI], in its current legal structure, is viewed as less likely to receive the multilateral endorsement required for enactment. Indeed, dating back to the Cuban Missile Crisis [October 1962], President Kennedy "meticulously crafted the 'quarantine' of Cuba…to minimize the risk that the Soviet Union would view the seizure of ships as an act of war" (Schulman 2006:22).

Network conflict as practiced today has precipitated a major change in combating one's enemy. Moreover, it is because asymmetric threats and terrorism are at the center of the cargo debate, that the efficacy of network centric methods is considered for review. Perrow's (2004) critique, in particular, recommends a radical decentralization—a new game, not a plan. In fact, decentralized networks work well because they adapt and innovate quickly when chance events, accidents, and failures occur. Overall, the research study exposed an integrated assessment of potential threats, vulnerabilities, and levels of risk to cargo supply chains (e.g. a 72-four delay *equates* to a global economic 'disaster'). Conceivably, a future terrorist scenario lies not with containers, but more likely with the instrumental use of an inflammable, set-adrift tanker(s) at a strategic chokepoint [e.g. Straits of Malacca, Bosporus, Hormuz or the Suez Canal].

One overriding issue that might substantially increase the command and control of potential threats would be a revamping of registry procedures for *Flags of Convenience.* As discussed in the paper, there are a number of controversial issues inherent in the use and misuse of *Flags of Convenience*; in particular, the lack of supervised regulation by an uncompromising, international agency. We argue that the failure to properly regulate registrations and monitor *Flags of Convenience* compound any workable network operation. Nonetheless, the extent of the risk could be reduced to acceptable levels, using a complex adaptive model to track *Flags of Convenience* ships and/or "shell" companies. The system would not however, hinder the free flow of global trade and commerce.

A major part of the paper addresses cargo security issues in the form of a Global Information Awareness Network: A collaborative environment made up of several components. For example, Complex Adaptive Systems [CAS] and Shared Awareness offer a much needed system of information sharing using a global network of investigative agencies. The nature of adaptation is inherent in its ability to 'exploit its environment' and thrive' (Grisogono 2004). Overall, the emergence of a maritime secure world--one that is indispensable to the global economy—and less vulnerable to disruptive threats--will depend on the manner in which public agencies respond to the threats. Finally, we need to manage our strengths in light of new, almost limitless power, not only to win battles in better and quicker ways, but also to preserve and improve human dignity in spite of machine efficiency.

References

American Behavior Scientist (2005) Vol. 48, No. 6: 683-699

Ahmed, R.Z. (2001) Osama hand in glove with LTTE *(The Times of India,* 2001 September 22)

Atkinson, S. R. and J. Moffat (2005) *The Agile Organization: From informal networks to complex effects and agility* Washington D.C.: CCRP publications series.

Bell, D.E. and LaPadula, L.J. (1976) *Secure Computer Systems:Unified Exposition and Multics Interpretation* ESD-TR-75306, MTR 2997 Rev. 1, The MITRE Corporation, March

Boisot , M. (2002) Information, Space, and the Information-Space: A Conceptual Framework. www.uoc.edu/in3/gnike/eng/docs/dp_02_boisot.doc

Broad, W.J. and Sanger, D.E. (2004) after ending arms program, Libya receives a surprise. *New York Times,* May 29

Brooks, M.R. and K.J. Button (2006) Market structures and shipping security , *Maritime Economics & Logistics*
Caryl, C. (2006) The box is king. *Newsweek* April 10-17 2006.

Chaffee D. (2003) Freedom or force on the high seas? Arms interdiction and international law *Nuclear Age Peace Foundation*: August 15. www.wagingpeace.org/articles

Clary, C. O. (2005) *The A. Q. Khan Network: Causes and Implications*. Master's Thesis Monterey, California: *Naval Post Graduate Schoo*

ComputerSecurity Institute (2005) CSI/FBI Computer Crime and Security Survey http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2005.pdf

Economist (2003). Peril on the sea 2 October

EUi Media (2004) US container screening system flawed-GAO www.E:%20Transport%20%20Transport

Flynn, S.E. (2006) Port security is a house of cards. *Far East Economic Review* January/February.

Friedman, T.L. (2005) *The World is Flat: A brief history of the 21st century* New York: Farrar, Strauss and Giroux

GAO (2003) Container security –Report to Congressional Requesters *US General Accounting Office* July

Gansler, J.S. and Binnendijk, H. (2004) Introduction: Information assurance overview. In Information Assurance: Trends, in vulnerabilities, threats, and technologies. Gansler, J. S. and Binnendijk, H. (eds.).

Getz, B. (2003) CIA pursues video game *The Washington Times*: September 29.

GLOBAL PIRACY REPORT (2006) IMB warns on new piracy hotspots in Annual Report. *Cargo Security* January 31.

Global Policy Forum (2005) A brief guide to flags of convenience www.globalpolicy.org

Greenberg, L.T.,(1998) Goodman, S.E. and Soo Hoo, Kevin J. Information warfare and international law. Unpublished paper.

Grisogono, A-M. (2004) What do national complex adaptive systems teach us about creating a robustly adaptive force? *9th International Command and Control Research and Teaching Symposium* –paper delivered; June.

Holland, J.H. (1995) *Hidden Order: How adaptation builds complexity* New York: Addison-Wesley

Joyner, D. H. (2004) The proliferation security initiative and international law, Athens, Georgia: CITS Briefs-University of Georgia.

Keohane, R. and Nye, J. (1971) *Transnational Relations and World Politics* Cambridge, MA: Harvard University Press.

Hofmann, S. (2004) Class of globalizations. In David Held and Anthony McGrew (Editors) *The Global Transformations Reader* Cambridge: Polity.

Lloyd, S. (2006) *Programming the Universe* N.Y.: Alfred A. Knopf.

Luft, G. and Korin, A. (2004) Terrorism goes to sea. *Foreign Affairs* November/December

McGuire, R. (2006) quoted in *Hard to Shock. Financial Times:* March 16

Mikkers, A. (2005) PricewaterhouseCoopers Global Economic Crime Survey 2005. Amsterdam November 29 http://www.pwcglobal.com/gx/eng/cfr/gecs/PwC_2005_global_crimesurvey.pdf

MOFA (2004) The Proliferation Security Initiative (PSI) maritime interdiction *exercise Ministry of Foreign Affairs of Japan.* October 2004.

Morse, E. (1971) transnational economic processes. In Keohane, R. and Nye.J. *Transnational Relations and World Politics* 23-47.

Perrow, C. (2004) Difficulties with network centric warfare. In Gansler, J. and Binnendijk, H. Editors *Information Assurance: Trends in vulnerabilities, threats, and technologies*

Pelkofski, J. (2005) Al Qaeda's maritime campaign www.military.com/forums December 27, 2005

Prefontaine, D.C. and Danduran, Y. (2004) *Terrorism and organized crime: Reflections on an illusive link and implications for criminal law reform*. International Society for Criminal Law Reform - Annual Meeting – Montreal, August 2004 - Security Measures and Links to Organized Crime

Riebling, M. (2004) The new paradigm—Merging law enforcement and counterterrorism strategies. Manhattan Institute
_________(2006) *Hard won lessons: The paradigm-Merging law enforcement and counterintelligence strategies*

Rehak, J. (2006) China is the center of a global boom in an increasingly strategic sector. *International Herald Tribune* 25-26 March.

Richardson, M. (2004) A time bomb for global trade: Maritime-related terrorism in an age of weapons of mass destruction. *Institute of South East Asia Studies "Viewpoints"* Pasir Panjang, Singapore: February 25

Roach, S. (2001) Back to borders, *Financial Times* September 28.

Sahm, C. (2006) Hard won lessons-Transit security

Scheuer, M., Ulph, S. and Daly, J.C.K. (2006) Saudi Oil Facilities *The Jamestown Foundation* May 2006

Schneier, B. (2000) *Secrets and Lies-Digital security in a networked world* New York: Addison-Wesley

Shazad, S.S. (2005) Armed and dangerous: Taliban gear up *South Asia Times on line* December 22, 2005.

Shulman, M.R. (2006) The proliferation security initiative as a new paradigm for peace and security *Strategic Studies Institute* http:// www.StrategicStudiesInstitute.army.mil/

Stankiewicz, W. (2005) International terrorism at sea as a menace to the civilization of the 21st century *American Behavioral Scientist,* Vol. 48 No.6 February 683-699.

Taylor, M.C. (2003) *The Moment of Complexity: Emerging network culture* Chicago: University of Chicago Press

USEU (2006) Container and cargo security *The United States Mission to the European Union* News April 15.

Virillio, P. (2002). Unknown Quantity. Paris: *Cartier Foundation*

Williams, P. (2003) Transnational Criminal Networks. In *Networks and Netwars: The future of terror* Crime and Militancy : RAND.
__________(2003) Transnational Criminal Networks and International Security In *Athena's Camp: Preparing for conflict in an information age*—RAND

Weick, K. (1995) *Sense-making in Organizations* London: Sage Publications.
________(1993) The collapse of sense-making in organizations: the Mann Gulch disaster *Administrative Science Quarterly, 38, 628-652.*
Woods, N. (2004) Order, globalization and inequality in world politics. In David Held and Anthony McGrew *The Global Transformations Reader* Cambridge: Polity.

Times India (2001) Police file charges against Laden, 21 August.

Wright, R. (2006) Maersk looks to terminal purchases to ease congestion *FT* March 29.

Van de Voort, M. and O'Brien, K.A. (2003) "Seacurity". Santa Monica, CA: RAND