NATO Individual Fellowship 1999/2001

FINAL REPORT

Strategic and Organisational Implications for Euro-Atlantic Security of Information Operations

Dr Andrew Rathmell

RAND Europe (www.randeurope.org)

&

Information Assurance Advisory Council (www.iaac.org.uk)

Abstract

The development of Information Operations and, more particularly, Computer Network Operations (CNO), has been paralleled by calls to control both the military and the criminal/terrorist use of these capabilities. The need for multilateral action to control criminal and terrorist activity is acknowledged and being pursued through mechanisms such as the Council of Europe. Efforts to control military use of CNO through arms control or multilateral behavioural norms are however being undermined by an unresolved dilemma faced by the leading powers; whether to exploit their CNO advantage for strategic purposes or to protect the global information environment on which depend. In resolving this dilemma, Western strategists need to take into account two important new features of the security environment – interdependency and the role of the private sector.

CONTENTS

1 Introduction

This paper is concerned with the prospects for the emergence of an international regime for control of Computer Network Operations (CNO). CNO are a subset of a broader set of malicious computer-mediated activities.

According to draft British military doctrine, CNO comprises: Computer Network Exploitation (CNE), namely: "the ability to gain access to information hosted on information systems and the ability to make use of the system itself;" Computer Network Attack (CNA), namely: the "use of novel approaches to enter computer networks and attack the data, the processes or the hardware;" and Computer Network Defence (CND), which is "protection against the enemy's CNA and CNE and incorporates hardware and software approaches alongside people based approaches."[1] In turn, CNO are one element of Information Operations (IO).

The precision of the military definition is not yet matched by internationally agreed definitions in the civil and criminal domains. The EU is now moving towards the concept of "cyber-abuse" as an overarching term to include activities ranging from privacy violations to attacks on computer systems.[2] The Council of Europe's Cybercrime Convention, with which EU approaches are likely to be harmonised, encompasses CNA under "category 1" offences, i.e. offences "against the confidentiality, integrity and availability of computer data and systems."[3] The G-8 Government-Industry Conference on High Tech Crime has however proposed that two major categories of threat be agreed upon, namely computer infrastructure attack and computer assisted threat. The former is defined as "operations to disrupt, deny, degrade, or destroy information resident in

[1] Ministry of Defence, *Draft doctrine for Information Operations; Joint Doctrine Pamphlet XX-01*. Joint Doctrine and Concepts Centre, Shrivenham, 1 March 2001, p. 8.
[2] http://www.jrc.deppv.it
[3] The other categories of offences are: 2) Computer-related offences; 3) Content-related offences; 4) Offences related to infringements of copyright and related rights.

computers and computer networks, or the computers and networks themselves. Malicious acts, unauthorized access, theft of service, denial of service."[4]

This paper does not seek to examine the details of any prospective regime or convention. Possible approaches using either criminal law[5] or arms control[6] have previously been examined in detail. Instead, this paper critically examines current approaches to the problem as embodied in the paradigms that dominate Western strategic thought. The paper argues that a more holistic understanding of the emerging global information environment[7] is required in order to better guide Western strategic interests and policy development.

The paper begins by framing the strategic dilemma of how to characterise and hence approach control of CNO, it then points to the "routinisation" of CNO within emerging NATO doctrine at the same time as multilateral efforts to secure cyberspace are gathering momentum. The paper then draws attention to the institutional disconnects that are hampering coherent Western policy-making before focusing on two central features of the emerging environment that are insufficiently accounted for by strategic policy-makers: interdependencies and the private sector. The paper concludes by arguing that Western strategic and economic interests can best be fulfilled by developing norms of military behaviour in cyberspace.

---

[4] G8 Government/Industry Conference on High-Tech Crime, *Report of Workshop 3: Threat Assessment and Prevention,* Tokyo, 22-24 May 2001, p. 1-2.

[5] Abraham D. Sofaer & Seymour D. Goodman, *A Proposal for an International Convention on Cyber-Crime and Terrorism*, Center for International Security and Cooperation, Stanford University, August 2000.

[6] See the conference organised by the Heinrich Böll Foundation, *Arms Control in Cyberspace: Perspectives for Peace Policy in the Age of Computer Network Attacks*, Berlin, 29 - 30 June 2001.

[7] The concept of global information environment is used here rather than the narrower concept of the global information infrastructure (GII). As today's GII evolves, the focus will shift from the Industrial Era concept of infrastructure protection/attack to the Information Age concept of information protection/attack. Britain's Defence Evaluation and Research Agency (DERA) coined the term "national digital environment" to replace the term NII. DERA*, An Analysis of the Military and Policy Context of Information Warfare*, June 1997, (DERA/CIS3/58/8/5).

2 The Strategic Dilemma

The central argument of this paper is that NATO states face an increasing tension between exploiting their CNO advantage in the military sphere and protecting the global information environment.

Led by the USA, NATO nations are moving apace to develop doctrines and capabilities that will allow them to exploit cyberspace for military advantage. Within the broad rubric of IO, increasing effort is being devoted to integrating Computer Network Operations (CNO) into routine military planning. At the same time, these nations are becoming increasingly concerned at the dependency of their militaries, governments, economies and societies on the networked information systems that are emerging as the nervous systems of post-industrial society. They are taking a range of actions, both unilaterally and multilaterally, to mitigate the resultant risks.

The desire both to exploit and to restrict CNO is a paradox that needs to be addressed before an international regime can be developed. Underlying this paradox are two divergent approaches to characterising the policy challenge.

2.1 Characterising the Problem

One approach defines the CNO threat as being from organised crime, electronic vandalism, corporate espionage and sub-state terrorism. The threat is defined as being to the economic prosperity and social stability of all nations plugged into the global information infrastructure. In this paradigm, all nations have an interest in working together to devise international regimes that will ensure the trustworthiness and survivability of information networks. It is a non-zero sum game.

From this perspective, a range of mechanisms can be used to mitigate the risks. International organisations can promulgate infosec standards and industry can be

encouraged to make its information systems more secure and dependable. International law enforcement mechanisms, such as Interpol, can be used for information exchange and investigations while multilateral conventions on computer crime, such as the Council of Europe convention, can be negotiated similar to those that deal with hijacking and other forms of criminality. While transnational investigations and traceback will always be a problem, at least the appropriate mechanisms exist through which such problems can be addressed.

The other approach treats control of CNO as a zero sum game. The focus is on the threat from nation states; IO and CNO are perceived as tools of strategic coercion. Although it may not be realistic to control CNE as an intelligence gathering tool, CNA that do breach the confidentiality, integrity or availability of information systems could in theory be treated as weapons of war and brought within the scope of arms control or the laws of armed conflict. In this approach, existing mechanisms and methods such as the Laws of Armed Conflict and arms control/verification regimes could be applied to this new "weapon system."

The contrast between these two approaches can be seen in the debate over the Russian UN General Assembly resolution that seeks to develop arms control approaches to IO and CNO. Russia's draft resolution, UNGA 53/70, called upon member states to "promote at multilateral levels the consideration of existing and potential threats in the field of information security" and requests progress on "developing international principles that would enhance the security of global information and telecommunications systems and help combat information terrorism and criminality."[8] Pointedly, Russia's submission to the UN Secretary General called for "acknowledgement that the use of information weapons against vital structures is comparable to the consequences of the use of weapons of mass destruction."[9]

[8] UN General Assembly, draft resolution 53/70, *Developments in the field of information and telecommunications in the context of international security*.
[9] *Note from Permanent Mission of the Russian Federation to the United Nations to the Secretary-General*, 9 June 1999, p. 4.

The important point is that the Russian submission was made to the General Assembly's First Committee, (dealing with disarmament issues). The USA has consistently urged that the matter be referred to the Second Committee (economic issues and financial matters) and/or the Sixth Committee (legal). This apparently abstruse bureaucratic point highlights the divergent paradigms in play.

2.2 Framing the Dilemma

The problem of how to treat CNO is recognised by the US military, which is at the cutting edge of military CNO developments.

A US Air Force sponsored workshop held in March 2000 concluded that international efforts to tackle cybercrime and cyberterrorism "could hinder US information warfare capabilities, thus requiring new investments or new research and development to maintain capabilities."[10] The dilemma was summed up in 1999 by the US Department of Defense whose legal counsel argued that:

> the United States has not yet addressed fundamental policy decisions about where its long-term interests lie in connection with the possible international legal restriction of information operations. On the one hand, there is an obvious military interest in being able to interfere with an adversary's information systems, …
>
> On the other hand, as the nation that relies most heavily on advanced information systems, the United States has the greatest vulnerability to attack. This concern would seem to drive U.S. policymakers to consider the merits of international restrictions on information operations.[11]

[10] USAF Directorate for Nuclear and Counterproliferation and Chemical and Biological Arms Control Institute, *Cyberwarfare: What Role for Arms Control and International Negotiations?,* Washington DC, 20 March 2000, p. 24.

[11] Department of Defense, Office of the General Legal Counsel*, An Assessment Of International Legal Issues in Information Operations*, May 1999.

That this policy dilemma remains unresolved is evident from the variety of activities in the Western world both in the military IO sphere and in the CND sphere, both civil and military. Whilst there is some coherence to current approaches, there is likely to be increasing tension between the multilateral institutions that are pursuing the military (offensive) and civil (defensive) tracks. An underlying problem is that existing state-led approaches to the military dimension of CNO fail to recognise the nature of the globally interdependent network environment and the leading role of the private sector in this domain.

3 Vertical Proliferation

Although great play is given by US defence analysts to potential CNO threats from nations such as China and Russia, it is the US, supported by its NATO allies, that is leading the way in turning CNO into a sophisticated and integrated strategic tool. Although CNO has played only a marginal role in recent operations such as Kosovo, the US and several NATO nations are moving to develop the capabilities, doctrines and organisational structures to operationalise CNO. Increasingly, IO is being regarded as "an integrating military strategy."[12] Within this context, NATO planners are routinising CNO as part of military planning, doctrine and capability development.

3.1 The US Leads the Way

The United States Army was the first branch of the US Armed Forces to publish a doctrine on Information Operations, back in 1996.[13] The doctrine was operationalised with assistance of the Land Information Warfare Activity (LIWA) during the tenure of Multinational Division North in peacekeeping operations in Bosnia. Lessons learned studies however demonstrated that an integrated doctrine, at the level of US forces, let alone that of a multinational coalition, was lacking. [14]

Whilst the US Air Force had deployed operational IW units at Kelly AFB and Shaw AFB since 1993, it was only in 1998 that USAF doctrine on IO, *Air Force Doctrine Document (AFDD) 2-5, Information Operations*, was released. In the same year, Joint Doctrine was also published under the authority of the Joint Chiefs of Staff. US Joint Publication 3-13 characterises Information Superiority (IS) as one of the cornerstones of US doctrine for the 21st century. IS is defined as "the capability to collect, process, and disseminate an

[12] Andrew Garfield, "Information Operations as an Integrating Strategy," in Alan d. Campen & Douglas H. Dearth, eds, *Cyberwar 3.0: Human factors in Information Operations and Future Conflict* (Fairfax, VA: AFCEA International Press, 2000), pp. 261-274.
[13] Department of Defense, *FM 100 – 6 Information Operations Doctrine*, Headquarters, Department of the Army Washington DC, August 1996 available at: http://www.adtdl.army.mil/cgi-bin/atdl.dll/fm/100-6/toc.htm
[14] LTC Garry J. Beavers & LTC Stephen W. Shanahan, "Operationalizing IO in Bosnia – Herzegovina," *Military Review*, Vol. LXXVII, No. 6 (November-December 1997).

uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." Within this framework, JP3-13 sets out the importance of an integrated use of IO in all aspects of a military operation.[15]

Joint and Air Force doctrine emerged in time for the 1999 Kosovo Campaign. Although the IO campaign against Serbia went a step further than the Bosnian campaign, there was still a lack of integrated planning and operations. As an element of IO, CNO and Special Information Operations (SIO) were used to only a limited extent. This was due to a combination of factors, including: lack of integration into overall campaign planning; uncertainty as to the legality of such operations; disagreement between intelligence and military personnel over whether to exploit or attack networks; unwillingness to expose US capabilities to the coalition; limited Serbian reliance on vulnerable networks.[16]

Further to this experience, in 1999 Computer Network Defence was handed to US Space Command (SPACECOM).[17] In October 2000, SPACECOM took over the CNA mission. The 609th Information Warfare Squadron was also moved to SPACECOM's area of responsibility.

3.2 The Europeans Follow

Leading European military powers have followed the US lead and are beginning to see IO (and CNO) as a routine part of their military operations. However, differences over definitions and limited resources to invest in new capabilities have meant that integration has been gradual and haphazard.

---

[15] Department of Defense, *Joint Publication 3-13, Joint Doctrine for Information Operations*, United States Joint Chiefs of Staff, Washington D.C., 9 October 1998, Ch IV, Information Operations Organization, pp. IV-1 available at http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf.

[16] http://www.airpower.maxwell.af.mil/airchronicles/apj/apj00/sum00/pounder.htm; Andrew Rathmell, "Information Operations: Coming of Age," *Jane's Intelligence Review*, May 2000.

[17] http://www.peterson.af.mil/usspace/new19-99.htm

The United Kingdom's 1997 Strategic Defence Review (SDR) recognised IO and CNO as a military activity of growing importance.[19] MoD recognised the advantages that digitisation could bring but pointed out that this created new dependencies which meant forces were much more susceptible to IO and CNA by malicious actors. Although the MoD carried out some elements of IO in the Kosovo campaign, it acknowledged in subsequent reviews that "our capabilities for conducting information operations need to be further developed."[20]

Since 1999, the UK's Joint Doctrine and Concepts Centre has been drafting a doctrine which is likely to be approved in late 2001. The draft doctrine defines IO as the military component of affecting the enemy's perception but points to the need for an integrated IO campaign to be coordinated across government.

France has been behind the United Kingdom in official development of organisational capabilities for IO. Although there have been speeches given by relatively senior figures in the French defence establishment, there have been no public statements that an IO doctrine is under development. Nonetheless, two research centres appear to be the focal points of French IO work. CELAR (Centre d'Electronique de l'Armament) specialises in the study of the application of IW techniques and the Ecole de Guerre Economique takes an interesting view of the application of IO by including economic vulnerabilities, as well as psychological warfare and information security. The main declaratory statements have been at conferences, where theories on the 'Mastery of Information' have been developed.[21]

German doctrinal thinking on the importance of IO in modern warfare was originally crystallised in a draft document entitled the *First Position of the German MoD on*

---

[19] Ministry of Defence, *Strategic Defence Review*, (London: The Stationary Office, 1998), p. 10.
[20] Ministry of Defence, Kosovo, *Lessons from the Crisis*, (London: The Stationary Office, 2000), p. 5; House of Commons, *Defence Select Committee Fourteenth Report*, (London: The Stationary Office, October 2000), Ch 3: "The Conduct of the Campaign: Information Operations," available at http://www.publications.parliament.uk/pa/cm199900/cmselect/cmdfence/347/34718.htm#a53.
[21] Jean-Pierre Meunier "Le CELAR, centre technique de la guerre de l'information", *L'Armement*, No. 60, Dec. 1997-Jan. 1998, pp. 84-88 & Col Jean-Luc Moliner, "La guerre de l'information vue par un opérationnel français", *L'Armement*, No. 60, Dec. 1997-Jan. 1998, p. 11.

InfoOps. A concept for IO is under development and is likely to be ready for political approval in the autumn of 2001. This concept paper, or Teilkonzeption bereichsübergreifende Aufgaben (TKBA) may well feed into the future overall Bundeswehr strategy Konzeption der Bundeswehr (KdB). While the current TKBA on IO has not been released, a 1999 Bundeswehr draft paper touched on CNO by referring to the importance of developing: "capabilities to manipulate, interrupt, compromise, ... an adversary's information and information systems."[22]

3.3 NATO Catches Up

NATO developed a draft policy on IO in 1997, based in part on a recognition of the crucial importance of this activity in the context of IFOR and SFOR. This policy defined IO as "actions taken to influence decision makers in support of political and military objectives by effecting the other's Information and/or Information Systems, while exploiting and protecting one's own Information and/or Information Systems."[23]

However, by the time of Operation Allied Force (OAF) in 1999, NATO had not moved from the conceptual stage to developing an agreed IO doctrine or to including IO in its exercises or planning. NATO planners recognised that their failure to implement an effective IO campaign reduced the effectiveness of OAF. They have acknowledged that "doctrine on information operations needs to be developed further."[24] A NATO doctrinal working group on IO was subsequently established but appeared to have made little progress by the summer of 2001. Nonetheless, NATO military planners recognise that IO will be used more and more in MOOTW (Military Operations Other Than War) where the 'centre of gravity' of allied and enemy forces will be psychological and therefore a prime candidate for CNO.

---

[22] Susanne Jantsch, "Comparative Approaches to Critical Infrastructure Protection - German Approach," presentation at *22nd National Information Systems Security Conference*, October 1999, Washington DC.
[23] MC 422
[24] Vice Admiral Haddacks, (UK Military Representative to NATO), *Minutes of Evidence to the Defence Select Committee*, (London: The Stationary Office, May 2000), available at http://www.parliament.the-stationery-office.co.uk/pa/cm199900/cmselect/cmdfence/347/0051704.htm
[25] *NATO, MC 402, Final Decision (Signed by LGen G.J. Folmer), Psychological Operations Policy, Sep 16, 1997)?? Get me this source please??*

At a higher level, the NATO Parliamentary Assembly has been discussing the issues of Information Warfare since 1997, when the Science and Technology Committee presented a report on Information Warfare and the Millennium Bug. In 1999, this same committee reported on 'Information Warfare and International Security'. The Committee argued that: "the possibility that the United States (or any other Western country) would develop and deploy offensive information warfare techniques has not been adequately discussed in public forums. This can be essential in order to build a national and possibly international consensus about the role of offensive information warfare and to clearly define its policies of use."[26]

[26] NATO, *Information Warfare and International Security*, NATO Parliamentary Assembly Science and Technology Committee, Brussels, 6th October, 1999 available at: http://www.naa.be/publications/comrep/1999/as285stc-e.html (visited 08/08/01)

4 Protecting Cyberspace

International businesses, governments and multilateral institutions have for some time been concerned at the implications of a growing reliance on information systems for critical business processes. In the past two decades, a variety of initiatives have been undertaken to improve the security and dependability of systems, of management practices and of international policing efforts. However, it was the rapid expansion of the Internet, of e-commerce and the promises of e-government in the 1990s that put security, reliability and privacy firmly onto the international policy agenda.

By 2001, European and US policy makers at the highest levels were expressing their concerns that insecure information systems threatened economic growth and national security. President Bush's National Security Adviser Condoleezza Rice noted in March 2001 that: "it is a paradox of our times that the very technology that makes our economy so dynamic and our military forces so dominating also makes us more vulnerable." She warned "Corrupt [the information] networks, and you disrupt this nation."[27] The European Commission warned in March 2001 that "the information infrastructure has become a critical part of the backbone of our economies. Users should be able to rely on the availability of information services and have the confidence that their communications and data are safe from unauthorised access or modification. The take up of electronic commerce and the full realisation of Information Society depend on this."[28]

As a result of these concerns, a complex and overlapping web of national, regional & multilateral initiatives has emerged.[29] A common theme behind these initiatives is the recognition of the inadequacy of existing state-centric policing and legislative structures to police international networks and the importance of ensuring that private networks are

[27] AP, "National Security Adviser sees cyberterrorist threat", 26 March 2001
[28] COM(2000) 890 final, *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*
[29] A comprehensive review of activities is presented in Rathmell, et al., *Information Operations: A Global Perspective* (Coulsden: Jane's Information Group, 2000).

secured against disruption. One way of grouping these initiatives is to use the standard information security paradigm of Deterrence; Prevention; Detection; and Reaction.

Deterrence: Multilateral initiatives to deter CNA include harmonising cyber-crime legislation to promote tougher criminal penalties and better e-commerce legislation (Council of Europe Convention, UNCITRAL).

Prevention: Multilateral initiatives to prevent CNA centre around promoting the design and use of more secure information systems (e.g. R&D initiatives between the US and EU; Common Criteria) and better information security management in both public and private sectors (e.g. ISO and OECD standards and guidelines initiatives). Other measures include legal and technological initiatives such as the promotion of security mechanisms (e.g. electronic signature legislation in Europe).

Detection: Multilateral initiatives to detect CNA include the creation of enhanced cooperative policing mechanisms (e.g. G-8 national points of contact for cyber-crime). Another important area is the effort to provide early warning of cyber-attack through exchanging information between the public and private sectors (e.g. US Information Sharing & Analysis Centres, FIRST, European Early Warning & Information System).

Reaction: Multilateral initiatives to react to CNA include efforts to design robust and survivable information infrastructures; development of crisis management systems; and improvement in coordination of policing and criminal justice efforts.

In toto, these initiatives involve significant investments of time and effort from a variety of government departments in many nations, from numerous international organisations and from numerous companies, large and small. Many initiatives are pre-existing, many are being pursued in isolation. Nonetheless, there has emerged a coherent and effective set of initiatives involving states and businesses, not to mention some NGOs, that is focused upon improving the security of the emerging global information environment.

5 A Joined Up Approach?

Upon surveying the parallel developments in the military (offensive) and defensive or protective spheres, an analyst could conclude that what we are seeing is a sophisticated twin track approach on the part of the leading global powers, notably the US national security community. Moreover, it is possible to understand the terms of the strategic debate in realist terms. As with any new military technology, the party that is most advanced wishes to retain that unilateral advantage by restricting opportunities for use of the capability against itself. Its potential adversaries will seek asymmetric responses.

The Bush Administration, which, at the time of writing is finalising a new national security approach within which to encapsulate Critical Infrastructure Protection (CIP), has been clear about its strategic vision. While it reinvents US armed forces for an era of Revolution in Military Affairs (RMA) operations, the Administration has made economic and homeland defence a priority. As the US seeks to make itself invulnerable from conventional threats by adopting RMA-era armed forces and from ballistic missiles through the National Missile Defence, its information infrastructure remains its soft underbelly. Hence, efforts to protect both the US infrastructure and those global infrastructures on which it is dependent are logical extensions of economic and homeland defence. The most effective way to stimulate defensive measures by government, industry and international organisations is to characterise the threat as coming from non-state actors, hence the hacker/cyber-terrorist paradigm.[30]

One asymmetric response to military weakness is to seek to use international legal instruments to restrain vertical proliferation on the part of a rival. Hence the Russian gambit at the UN. Russia's attempts to ban IO make strategic sense and mirror its efforts to restrict nuclear weapons in the early years of the Cold War. Russia recognises that, as it struggles to rebuild its economy, it is vulnerable to the advanced tools and doctrines of

IO that its Western rivals are developing. Unable to counter in kind, or to afford comprehensive defensive measures, Russia is seeking to use international law to reduce America's military advantage.

Another response is indicated in recent Chinese military writings. The widely-quoted People's Liberation Army (PLA) publication *Unrestricted Warfare* makes the point that emerging international norms and rules are shaped to fit the interests of the USA. Therefore, a weaker power must subvert these rules. This goes for operations in cyberspace as much as in other spheres. As the book puts it: "strong countries make the rules while rising ones break them and exploit loopholes . . .The United States breaks [UN rules] and makes new ones when these rules don't suit [its purposes], but it has to observe its own rules or the whole world will not trust it." Therefore, "the first rule of unrestricted warfare is that there are no rules, with nothing forbidden."[31] Thus, a weaker power should realise that: "all these non-war actions [hacking, financial manipulations, perception management] may be the new factors constituting future warfare."[32]

Unfortunately, if strategists in Western capitals, mirrored by their counterparts in Moscow and Beijing, believe that they are merely engaging in the time-honoured game of seeking strategic advantage from a new technology, they fail to perceive crucial elements of the new environment in which they are operating. The problem is that both sides of the argument are working within a set of paradigms that are outdated in the globalised and networked world. The most important aspects that are being missed are the nature of interdependency and the role of the private sector.

Before elaborating on this point, it is worth noting that, even within the current paradigm, there are serious inconsistencies in both institutional and conceptual terms that are undermining Western policy.

---

[30] Nonetheless, Western security agencies are really concerned about foreign state CNE and potential CNA which they see as having much greater capabilities in the longer term.

[31] Editors note in forward to Qiao Liang & Wang Xiangsui, *Unrestricted Warfare*, (Beijing: PLA Literature and Arts Publishing House, February 1999), p. 2.

5.1 Multiple Agencies, Multiple Agendas

On an issue as complex as CNA/CND, which cuts across so many traditional bureaucratic and sectoral boundaries, it is not surprising that there are institutional schisms. Underlying the institutional issues, however, are questions of the extent to which policy-making is really joined up and, hence, intellectually coherent.

In simple institutional terms, it is evident that it is the military and national security institutions in the USA and its allies that are pursuing the development of CNO. It is the civil government/commerce and law enforcement institutions that are devising and implementing defensive policies.

Clearly, within countries, there is some involvement by the military in protection of national infrastructures. Indeed, the military drove much of this original work as they were concerned at their dependence on insecure civil infrastructures. Nonetheless, the military role has declined since the late 1990s as the focus has shifted to the private sector and to civil government agencies.

The institutional schisms at the multilateral level can be seen most clearly in the form of NATO and the EU. For the purposes of this argument, the membership of the two groupings can be regarded as overlapping. Apart from the fact that the leading European players in CNO and CIP are in both organisations, the USA also has an growing role in EU deliberations on cybercrime and network security.[33]

Despite this overlap in membership and an obvious shared interest in protecting NATO and EU networks, the policy agendas being pursued are radically different. NATO is seeking to legitimise and routinise CNO as a military instrument of coercion. The EU is seeking to delegitimise cyber-attacks and to build robust global information networks that will make cyber-attacks harder to conduct, easier to trace and easier to recover from.

---

[32] Ibid, p. 12.

[33] For instance, the US Department of Justice played an important role in the development of the Council of Europe Convention and the US State Department and defence research community have growing links to the European dependability R&D community.

A conspiracy theorist, or believer in government as a rational actor, would argue that this represents a sophisticated, multilateral sword and shield approach in which NATO forges the CNO sword and the EU deploys the CND shield. In this case, however, the cock up theory holds more water than the conspiracy theory. NATO and the EU represent different bureaucratic constituencies which are often not joined up at home. Whilst NATO discussions on CNO involve primarily the military, with support from intelligence agencies, EU discussions on dependability and cybercrime involve commerce ministries and law enforcement.

The translation of institutional disconnect into incoherent policy is not just a potential problem. A good example of the problem on the domestic scene was found in recent UK legislation. In short succession, the Department of Trade & Industry sponsored a minimalist, pro-business Act promoting e-commerce (Electronic Communications Act) whilst the Home Office sponsored the regressive and intrusive Regulation of Investigatory Powers Act. Unfortunately, the consequences of policy incoherence and of divergent agendas at the multilateral level undermine the framework of trust upon which the emerging global Information Society is being built.

6 An Interdependent World

Of the two elements of the global information environment paradigm that are missed by Western strategists, it is the notion of interdependency that current military thinking on CNO most fails to appreciate. In short, there is a disjunction between the technological and market realities of a globalised, interdependent and networked world and emerging military doctrine on IO and CNO. Constrained by a focus on delivering "effect" to a particular geographic conflict zone and within existing "kinetic-era" legal paradigms, militaries are trying to exploit CNO for precise targeting of enemy infrastructures.

Unfortunately, the attempt to squeeze CNO into existing conventional force paradigms misses important truths about the *emerging* global information environment. It is not enough to devise military policy for today's rather rudimentary cyber-environment, it must take into account the next generation Internet and information environment that will emerge over the coming 5-10 years. The Next Generation Internet that will form the backbone of this information environment will provide always on connection through multiple devices embedded in all aspects of business, public and personal life.[34] Online computing will be pervasive.[35]

As today's Internet evolves into the Next Generation Internet (NGI), businesses, consumers and governments will depend upon the Internet even more than they do today. The Internet will become as ubiquitous as electricity and will have to be as reliable. With the advent of mobile computing and the micro applications of Information Technology, concepts like IBM's Intelligent Kitchen will be realised. This envisages an environment in which even household appliances are connected to 'the Grid' and where devices use networked information technology in a pervasive and ubiquitous manner to find and use services as and when they need them. In this way the whole Internet melts into one giant

[34] For instance, the advent of Personal Area Networks (PAN) will embed the human user firmly within the Internet infrastructure.
[35] Global Internet Project, *A Primer On The Security, Privacy and Reliability of the Next Generation Internet* (6 November 2000).

computer. This means that the Internet will be not only interdependent, but super–dependent.[36]

Three aspects of this future environment are of particular significance:[37]

> High powered, embedded computational capability will become pervasive in the civil sector. … localised wireless communication devices will dominate the consumer electronics sector within the next 5 years. This will become an enabling technology for the wide-scale adoption of … "ubiquitous computing". This … will dramatically increase the level of connectivity and lead to new, ill understood, systems behaviour.
>
> The emergence of a highly connected Global Information Infrastructure (GII)[38] with converged broadband computing, media, telecommunications capabilities … will greatly complicate interdependency analysis.
>
> Greater interconnectivity between traditionally separate information infrastructures may drastically alter overall systems behaviour. Particularly worrying is the potential emergence of infrastructures with in-built instability, critical points of failure, and extensive interdependency.

6.1 The Blowback Effect

These features of the emerging information environment make it extremely unlikely that any but the most limited and tactically-oriented uses of CNO could be contained as called

[36] "Computing Power on Tap"*, The Economist*, 23 June 2001

[37] Abstracted from IAAC, *Information Assurance & Security Research & Development Policy Paper*, July 2001 available at http://www.iaac.ac.uk.

[38] The GII can be defined as "that system of advanced computer systems, databases and telecommunications networks … that make electronic information widely available and accessible. This includes the Internet, the public switched network and cable, wireless and satellite communications." Adapted from definition of NII in: US Senate Permanent Subcommittee on Investigations, Hearings on "Security in Cyberspace," 5 June 1996.

for by current military doctrine. There are a number of ways in which military use of CNO could "blowback"[40] on Western societies through the interdependencies that will characterise the new environment.

The most obvious route is through direct network interdependencies. Even in today's environment, relatively innocuous cyber-weapons such as viruses and worms "in the wild" can cause considerable disruption to businesses, governments and consumers. This risk is parallel to that with Biological Weapons, any use of which has always faced the risk of infecting friendly populations.

Another "blowback" channel is via second and third order dependencies. In today's globalised, liberalised and just-in-time economy, governments and companies have found it almost impossible to map and understand their wider dependencies.[41] As the discussion above highlights, the emerging information environment is likely to exacerbate these interdependencies and to make systems behaviour even harder to predict. The most sophisticated attempt yet to model these interdependencies, by the US Department of Energy, is increasingly turning to chaos theory for assistance in its task. Against this background, Western militaries cannot responsibly claim to be able to predict the knock-on effects of large-scale CNO use in the context of a wired world.

A more intangible blowback effect is that the routine use of CNO risks undermining trust in cyberspace. Across the developed world, a lack of trust and confidence in information networks is already a barrier to the rapid take-up of e-commerce and e-government. Trust is being undermined by cyber-vandals (hackers and virus writers), by cyber-criminals, by cyber-espionage[42] and by companies that abuse online privacy. The knowledge that global information networks are being routinely exploited by Western

---

[40] Peter Feaver, *Information Warfare and the Political Control of Coercion* (Duke University, Durham, 1997), p. 16.

[41] The fuel crisis that almost brought the UK to a halt in 2000 is a good example of these interdependencies, if in the physical world.

[42] For instance, see European concerns over "Echelon". Temporary Committee on the Echelon Interception System, *'Draft Report on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON Interception System)*', European Parliament, Brussels, 18th May 2001. http://www.europarl.eu.int/tempcom/echelon/pdf/prechelon_en.pdf

militaries would lead users to question whether data and systems were trustworthy and whether information was being polluted. The damage to consumer and business confidence could well undermine efforts to promote a trusted Information Society.

Finally, another intangible effect has already been considered by the US military. For the US, one reason for not using IO more aggressively in the Kosovo conflict was the fear that this could set a legal and operational precedent. Routinisation of CNO as a military tool by NATO states will remove any legal, political or operational barriers to its routine use by other states and groups. Given that the balance in CNO is likely to favour the offence for some time to come, it is not at all clear that the routine adoption of CNO would be in the West's strategic advantage.

7 Bringing in Business

The other element of the new paradigm is the increased part played by the private sector.[43] Policy-makers dealing with CIP have come to recognise that defensive policies are untenable without active participation by the private sector since this sector owns and operates the networks and knows what is going on in cyberspace. The USA is addressing this problem by inviting industry to participate in writing its National Plan for Infrastructure Protection. The European Commission explained the problem succinctly:

> whilst security has become a key challenge for policy makers, finding an adequate policy response is becoming an increasingly complex task. Only a few years ago, network security was predominantly an issue for state monopolies …. Establishing a security policy was a relatively straightforward task. This situation has now changed considerably because of a variety of developments in the wider market context, amongst them liberalisation, convergence and globalisation
>
> … these developments constrain the ability of governments to influence the level of security of the electronic communications of their citizens and businesses.[45]

The recognition of the central importance of the private sector in the formulation and implementation of policy in this domain has long been recognised in some multilateral fora, such as the OECD.[46] There is however a long history of clashes between states' perceptions of their national security needs and of businesses' perceived needs to secure their international operations.

[43] Taken here to mean primarily private business but also NGOs and individuals as users of networks, as citizens and as consumers.

[45] *Network Security Communication*, pp. 3-4

7.1 A Troubled Past

The debate over cryptography policy provides the most obvious examples of these clashes. In the 1990s the use of cryptography spread from a few specialised, civil applications such as banking and Western governments became concerned about the impact of widespread, strong cryptography on their intelligence activities. The business view was that strong cryptography was vital for the success of e-commerce and the growth of the Internet. Civil liberties groups supported liberalisation in the name of privacy. The US government however sought to control the proliferation of strong cryptography, arguing that putting cryptography into the hands of criminals would make the tasks of law enforcement much harder.[47] European governments took varying views.

Throughout much of the 1990s the US government engaged in various efforts to control cryptography, to ensure that weak crypto was used at home and abroad and to ensure government retained access to encryption keys. The Clipper Chip was the most notorious but key escrow mechanisms such as Trusted Third Parties were intensively discussed. In Europe there were both very restrictive policies (e.g. France) and more liberal approaches (e.g. Ireland and Belgium).

On the multilateral level, the issue was dealt with through the Wassenaar Arrangement, the 33 nation successor to COCOM that was founded in 1996. Wassenaar imposes controls on exports of dual-use goods and munitions; including certain encryption products. It declares that "the export of encryption technology will remain possible without depositing keys with government agencies" but that asymmetric encryption procedures appearing under the dual use list, category 5, part 2 (Information Security) are

[46] For instance, the Business & Industry Advisory Council was extensively involved in the development of OECD *Guidelines for the Security of Information Systems.*

[47] Though, as Ross Anderson argues, the primary motivator for the position of the US Government was concerns over national security intelligence collection rather than criminal intelligence collection. Ross J. Anderson, *Security Engineering: A guide to Building Dependable Distributed Systems* (Chichester: John Wiley & Sones, Inc, 2001), pp. 461-464.

restricted.[48] The debate has been over the strength of the encryption allowed, measured in bits.

By the end of the 1990s, the debate had shifted in favour of liberalisation. As a 1996 report by the US National Research Council concluded, "on balance the advantages of more widespread use of cryptography outweigh the disadvantages."[49] In 2000, the Clinton administration revised export regulations on high grade encryption, permitting exports to EU member states and Australia, Czech Republic, Hungary, Japan, New Zealand, Norway, Poland and Switzerland without a government license.[50] This paved the way for Wassenaar restrictions to be lifted from 56 bits to 512 bits, meaning that everything but extremely sophisticated military encryption was liberalised. This harmonisation of international approaches was reflected in individual European states; even France made a dramatic U-Turn and adopted an approach of almost complete liberalisation. [51]

Whilst this shift in policy did to some extent represent the victory of the views of business and civil liberties campaigners over those of national security establishments, the debate is far from over. For instance, the EU's directive on electronic signatures was only finally concluded once state and business parties to the negotiations had agreed to focus on one application of cryptography – authentication – rather than to include confidentiality. The problem of how to ensure that strong encryption for confidentiality does not undermine law enforcement intelligence efforts remains undecided. The UK's Regulation of Investigatory Powers Act uses legal sanctions to ensure "escrow by intimidation"[52] The Council of Europe Cybercrime Convention adopts a similar model.[53]

---

[48] List of Dual Use Goods and Technologies And Munitions List * WA LIST (00) 1 01-Dec-00 Category 5 Part 2 – Information Security available at: http://www.wassenaar.org/list/Cat%205P2%20-%2099.pdf

[49] Brian Gladman, *Wassenaar Controls, Cyber-Crime and Information Terrorism,* Cyber Rights and Cyber Liberties (UK), London, September 1998 available at: http://www.cyber-rights.org/crypto/wassenaar.htm

[50] http://www.bxa.doc.gov/Encryption/19Oct2KFactsheet.html

[51] Assemblée Nationale, Document no. 314, *Projet de Loi sur la Societe de l'Information*, Assemblée Nationale, Paris, 14 June 2001 available at: http://www.assemblee-nationale.fr/projets/pl3143.asp

[52] Anderson, p. 467.

[53] "[Each Party shall] adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary

7.2 A Clouded Future

The crypto debate has in part been resolved in favour of business but serious differences remain between states and businesses. As CNO becomes a more prominent issue, it is likely that a new source of tension will emerge between states and businesses.

This time, though, government strategists on all sides will find it much harder to enforce their positions on the private sector. The fact that the private sector now leads in developing, deploying and operating the information networks in question poses challenges both to states such as the USA who want to exploit CNO and to states such as Russia who seek to control this capability.

Insofar as military exploitation of CNA is concerned, there is a growing recognition by businesses who are becoming reliant on the global network of networks that the fragile commodity of trust could all too easily be undermined by military uses of CNO. Even if individual global or Western businesses are not the direct targets of CNA in a military campaign, the potential for knock-on effects as outlined above is disturbing. In the debate over key escrow, a central concern of business has been that even the *perception* of the *possibility* that data could be accessed by a third party such as a government could undermine trust in e-commerce. The same argument applies many times over if information networks are routinely exploited by NATO militaries for purposes that will, necessarily, remain undisclosed.

As for those who seek to limit CNA proliferation, the arms control community has a problem in that state centric arms control approaches have traditionally not had to engage with business, except in a prescriptive manner through export control regimes e.g. (MTCR, NSG). The Chemical Weapons Convention (CWC) and the Biological Weapons Convention (BWC), both of which deal with dual-use goods in a globalised

---

information, to enable [authorities to access stored computer data]" Council of Europe, *Draft Cyber-Crime Convention,* Committee of Experts on Crime in Cyber-Space (PC-CY), Strasbourg 29th June 2001, Article 19.4 available at: http://conventions.coe.int/Treaty/EN/cadreprojets.htm

54

industry, provide both positive and negative lessons for any arms control initiatives in this sphere. As will be discussed below, though, the conceptual and practical problems in designing an arms control regime for CNA are much more complex.

8 Developing Norms

If the proliferation and routinisation of military CNO pose a danger to the information society, then it is important to examine ways of limiting the vertical and horizontal proliferation of CNO. Before outlining possible approaches, it is worth addressing the common argument that the current structure of the international system will void any such effort.

8.1 Power Politics

Surely, it is commonly argued, the US "hyperpower" will not agree to have its hands tied by its rivals and by idealistic arms controllers. There is little point developing norms and regimes for controlling CNO if a convincing argument cannot be made to US strategists that these may, in fact, be in US national security interests.

In fact, such an argument can be made. While there is a clear strategic advantage to the US to remain the dominant power in the field of IO and CNO, it is not in US strategic interests to allow the unfettered proliferation and use of CNO, even if the US retains the offensive lead. An obvious reason is US national vulnerability to CNA. It remains a moot point and the subject of numerous wargames whether unconstrained use of CNO in a future conflict would be to the net benefit of the US. Rather, widespread use of CNA may give opponents an asymmetric tool by which to undermine the US's conventional, nuclear, economic and diplomatic might. As John Arquilla has argued, it is in the USA's strategic interests to pursue cyber-arms control as "we are such a broad and rich target."[55]

More fundamentally, however, by engaging in the building of norms that restrict the use of CNO, the US will be able to use its leading military and technical position to shape the international agenda, customary law and practice and to lay out the bases of discussions. As Neal Pollard has argued, it would be in the interests of the US to adopt an open

[55] Stephen Green, "Pentagon Giving Cyberwarfare High Priority," *Copley News Service*, 21 December 1999.

declaratory policy on strategic CNA in order to raise the deterrent threshold. A unilateral declaratory policy would provide "a nexus around which the international community can consider strategic CNA in conflict, perhaps providing a starting point for a normative framework."[56]

8.2 Arms Control

Although arms control approaches to controlling CNO have begun to be discussed, it is hard to envisage traditional capability-based arms control being of much utility due to the impossibility of verifying limitations on technical capabilities possessed by a state. As Anders Eriksson put it: "generally speaking, the avenues available for "arms control" in this arena are primarily information exchange and norm-building, whereas structural approaches—trying to prohibit the means of information warfare altogether or restricting their availability—are largely impossible due to the ubiquity and dual-use nature of information technology."[57]

The CWC and BWC have also dealt with dual-use technology but the current struggle to develop a verification regime for the BWC indicates some of the problems that would be faced by any cyber-arms control verification regime.[58] While it is true that the creation of organised military IO/CNO units could be monitored with the assistance of Western intelligence services, the proliferation of CNA capabilities in themselves could not really be monitored since the technology required (hardware, software and "wet-ware") is inherently globalised. The fact that existing multilateral and national arms control regimes are only beginning to grapple with the export of intangibles such as software and know-how[59] indicates how difficult any controls would be in an era when cyber-attack scripts reside on Internet hosts computers around the world.

---

[56] Neal Pollard, "The Mouse that Leaves Something to Chance: Deterrence and Computer Network Attack," unpublished draft paper, 2000, p. 49.
[57] E. Anders Eriksson, "Information Warfare: Hype Or Reality?," *The Non-Proliferation Review*, Spring-Summer 1999, Vol. 6, No. 3.
[58] "Bugs in the system," *The Economist*, 16 June 2001.
[59] House of Commons, *Export Control Bill,* (London: The Stationary Office, June 2001) available at: http://www.publications.parliament.uk/pa/cm200102/cmbills/005/2002005.pdf

Even if approaches to cyber-arms control could be conceived and verification regimes designed, arms controllers would face two enormous challenges. First, even more than with the BWC, any regime would need the involvement and support of the private sector from the start. The globalised Information & Communications Technology (ICT) industry is not one to which top-down mandatory regulations can easily be applied, unlike, for instance, the more traditional, nationally-based defence manufacturers.

The other key problem would be the need to ensure that restrictions on state proliferation did not disadvantage states vis a vis sub-state groups. Given the potential that CNO provide for sub-state groups to wreak serious damage on states, multilateral controls on sub-state and criminal behaviour would have to be reinforced before states are likely to accept controls on their own capabilities.

8.3 Norms and Codes of Conduct

Whilst arms control may not be a feasible approach for the time being, an approach that seeks to develop norms of use and non-use is certainly worth exploring. The aim of developing explicit norms of behaviour would be to govern the new risks by making behaviour more predictable and so enhancing business and citizen trust and confidence. The case for norms was made by Jack Mendelsohn, speaking to the NATO Parliamentary Assembly in May 2000, "if we were to … drift toward an increasingly opaque world, without structure, without norms and without predictability, where nations would be seeking unilaterally to ensure their own security, how could you hold out any hope to your constituents for a more peaceable, stable and secure world."[60]

These norms may well include definitions of when and how CNO could be used (for instance as part of enforcement mechanisms under UN auspices). This debate would have to take careful account of the "blowback" risks identified above but could thereby ensure that some of the perceived military advantages of CNO were exploited in the

[60] J. Mendelsohn, "Does Arms Control Have a Future?," NATO Parliamentary Assembly 46th Rose Roth Seminar, *Non-Proliferation and Arms Control: The Agenda for the 21st Century*, Portoroz, Slovenia - 4/6 May 2000.

interests of the international community rather than for, destabilising, unilateral advantage.

Norms for CNO are, by default, already being developed by the leading powers. As they develop their IO doctrines, NATO militaries are examining existing legal restrictions on use and restrictions on targeting under the Laws of Armed Conflict.[61] Information Warriors are seeking to ensure that IO and CNO meet the classic requirements of military necessity, humanity and chivalry. There is also a vibrant debate over the extent to which cyber-attacks can be classed as armed attacks under international law and the terms of the UN Charter.

Efforts have also been made in multilateral for a to develop norms that could put NATO doctrine into a wider context and influence the global development of IO and CNO capabilities. The most significant effort has been within the EU, where Germany, Sweden and Austria jointly sponsored efforts to apply military codes of conduct to IO. Although the initiative was reportedly blocked by the UK, this route retains a great deal of potential.[62] Codes of conduct are used within the OSCE to encourage harmonisation of military practice and civil-military relations across OSCE member states, notably in the former Eastern Bloc.[63] Codes of conduct provide a mechanism by which states with current IO capabilities can ensure that both their own use of IO/CNO and that of future proliferators will be regulated and within agreed boundaries.

If the development of codes of conduct is to be successful, however, four factors need to be integrated into the process as soon as possible.

---

[61] Richard W. Aldrich, *The International Legal Implications of Information Warfare* (Colorado Springs: US Air Force Academy, 1996); Mark Russell Shulman, *Legal Constraints on Information Warfare* (Maxwell Air Force Base, AL: Air University, 1999).
[62] Johannes Bertholdt, *Arms Control in Cyberspace*, Department of Arms Control, Federal Ministry of Foreign Affairs, Berlin, 29 June 200 available at: http://www.boell.de/downloads/medien/bjohannes.pdf
[63] OSCE, *Towards a Genuine Partnership in a New Era – Decision No IV; Code of Conduct on Politico – Military Aspects of Security*, Budapest Document 1994, adopted at the Budapest Summit 1994, Budapest, 6 December 1994 available at: http://www.osce.org/docs/english/1990-1999/summits/buda94e.htm#Anchor_COD_65130

First, any norms and restrictions must be developed in light of the likely future market and technological environment. It will be important to understand the risks outlined in section six above and to ensure that the norms are framed broadly enough to be frequently updated since CNO will not be carried out within a stable and predictable environment.

Second, advantage should be taken of likely harmonisation within OSCE member states and indeed globally as multilateral initiatives on CND and CIP progress. In the short term, EU associate nations are likely to be engaged in EU efforts to secure regional information infrastructures. In the longer term, legal and other measures are likely to move towards global harmonisation as more countries join the fight against cyber-crime. Since the defence is inseparable from the offence, defensive harmonisation can advance convergence on norms for offensive operations.

Third, advantage should be taken of emerging plans for internationally coordinated Alert, Warning and Response (AWR) systems to counter cyber-attack. The G-8, EU, USA and international policing and industry groupings are making progress towards the development of standardised and integrated systems to ensure detection of cyber-attacks.[64] These systems can contribute to the verification and enforcement of norms since most nations will be subject to network monitoring and reporting.

Fourth, and perhaps most importantly, the private sector needs to be engaged up front in development of any norms or codes of conduct. The necessity of engaging the private sector in policy development is recognised in the field of CIP and domestic CND. However, in a multilateral context, businesses and NGOs must be given a central role since they understand the infrastructures, are already setting international standards and are designing alert and warning systems.[65]

[64] Andrew Rathmell, "Building Partnerships to Protect Europe's Infrastructures," *Information Systems Security Europe Conference,* London, 28 September 2001.
[65] "What's in a Scan?" *Canadian IO Bulletin*, Vol. 2, No. 2 (June 1999).

9 Conclusion

The benefits of e-government, digitised battlespaces and e-commerce are evident to the advanced nations; less developed states also recognise the importance of plugging into the emerging global information environment. It is equally evident that, without trustworthy systems and survivable infrastructures, the information revolution will not progress. Hence an increasing number of governments are grappling with the problem of building secure electronic commerce environments and of ensuring protection of their critical national infrastructures.

America and its strategic partners will have to decide how they wish to balance contradictory requirements. On one hand it is in their economic and security interests to see the emergence of robust international conventions and mechanisms that protect the global information environment. On the other hand, their investment in military technologies and doctrines designed to disrupt the infrastructures of rival nations is a comparative strategic advantage that they will be loath to give up. Nonetheless, there is a strong argument that it would be to the overall strategic benefit of the Western powers to accept internationally agreed norms of use for CNO.

As with cryptography, the particular interests of warfighters and intelligence agencies do not outweigh the broader societal benefits of a secure information environment. The adoption of multilateral norms such as codes of conduct provides one way ahead. To be effective, such norms must be designed with an eye to a dynamic future and must engage the private sector from the start.