IWS –The Information Warfare Site
Infocon Magazine Issue One, October 2003
http://www.iwar.org.uk/infocon/

MEASURING 'DIGITAL WARS': LEARNING FROM THE EXPERIENCE OF PEACE RESEARCH AND ARMS CONTROL

Giampiero Giacomello
Department of Political Science
University of Bologna, Italy

email: giacomel@spbo.unibo.it

Abstract

Are 'digital wars'(or, Computer Networks Operations in military-speak) 'real'? Can they really cause economic damage and loss of lives? Can poor countries use them to integrate or even, following Sun Tzu, to replace more expensive weapons systems? If the answers are positive, then it should be possible to measure cyberwars. In democratic countries, it should be even possible to compare different measurements and include the public in an open discussion. But research on digital wars takes place in closed laboratories and feeding public opinion with unverifiable data and the media with "ad hoc" anecdotes seem common developments in several countries.

This exploratory research offers an index to measure a type of information war as well as some suggestions on why a public debate on this crucial issue is necessary and how it might proceed. It does so relying on the experience of arms control and peace research scholars that during the Cold War had to face the same obstacles.

Measuring 'Digital Wars'[ψ]

Are digital wars (or "infowars" or Computer Networks Operations, CNO)[1] a possible occurrence or just a myth? Can they be measured so as to answer this question? And if so, how? To address these questions, the first goal of this paper is to put forward a scale to rank a type of CNO capability of several countries. The second is to offer a critique of an interpretation of digital wars, which seem to enjoy considerable popularity among the media and academia alike. The third, and perhaps most ambitious, goal of this research is to advance some hypotheses to answer the question "why did the question about the true 'nature' of digital wars (myth or reality), in the first place, emerge?"

Scholars have only recently begun to tackle the issue of accurately measuring CNO. These circumstances reduce the prospect for comparison with several other

---

[ψ] The bulk of this article was written while I was 2002 Summer Fellow with the Information Technology, Global Cooperation and International Security (ITIC) Program at the Social Science Research Council in New York. I would like to thank Johan Erickson, Ralf Bendrath, "Gus" Hosein, Dorothy Denning, Lucio Picci, Wanja E. Naef and Brenda Coughlin for their suggestions, ideas and criticism.

[1] Digital wars can be seen as a specific type of information warfare (IW). The term "information warfare" has now been applied to a rather dissimilar (and often incongruent) collection of situations. Its origins can be traced back to the Gulf War, when the UN coalition simply annihilated Iraq's information systems (see for instance Campen, 1992). The official US Department of Defense (DoD) definition of IW, or, more precisely, Information Operations (IO), is "*actions taken to affect adversary information and information systems* while defending one's own information and information systems" (DoD, 1998: vii; emphasis in the original). The current use of the term, however, has come to include "precision-bombing of enemy's information infrastructure", cyberterrorism and cybercrime, "script-kiddies" (i.e. unskilled young individuals that download ready-to-use software from the Internet) practicing denial-of-service (DoS) attacks on commercial Web sites, Web defacement, etc. Libicki (1995) identified seven "forms" of IW, of which cyberwar is only one. In an effort to clarify the matter, Arquilla and Ronsfeld (2001) have recently distinguished between "cyberwar" and "netwar"—the latter being waged by Networksed organizations such as terrorist groups, whereas the former are more in the realm of the state's actions. However, the tendency among NATO's military is now to distinguish between Computer Networkss Attacks (CNA) and Computer Networkss Defense (CND, also called Information Assurance, IA), which are both part of the general category of Computer Networkss Operations (CNO). The present plethora of various "e-something" (e-jihad, e-intifada, electronic Pearl Harbor, electronic Waterloo, etc.) is both confusing and meaningless, and is of immediate use only for the media, who tend to consider all these terms rather fungible (thus contributing to generating confusion). Henceforth, I will use the more precise term "CNO" then the more generic "digital wars", since my focus is on *computer Networkss* operations (hence I do not consider cases such as surgical

studies that would help to refine one's own analysis and direction of research. For this reason this research remains *exploratory* in character and cannot advance claims of causal explanation. Nevertheless, in the conclusions of this article, I will offer some room for discussion about the possible responses to my third question as well as a plan for future research.

In many respects, this article follows (a) an established pattern in social science research, that is to identify viable indicators to measure social phenomena and (b) a long-standing tradition, originated during the Cold War, of arms control and peace research studies. The former includes examples such as Taylor (1972), Russett et al. (1977), Horn (1993), or, more specifically, Dunnigan and Bay (1991, especially chapter 16).

The latter aimed to provide dependable data and analysis as counterbalance to the views expressed by national security communities and military analysts around the world. As one observer put it, it has been a traditional mission of peace research of providing independent data to the interested public and policy-makers and to have some counterweight to the military perspective.[2] For instance, in the late 1980s, one observer noted that the Stockholm International Peace Research Institute (SIPRI) probably contained more arms control experts than any other single center outside the US government (Robertson, 1987: 289).[3] These circumstances would hence allow for a richer and more comprehensive public discourse on security issues.

---

strikes against enemy's command and control centers) and on affecting national information infrastructures.

[2] I owe this point to Professor Harald Müller, director of the Peace Research Institute Frankfurt (PRIF) and long-time member of the peace research community.

[3] In this article I follow Robertson's (1987: 243) view that arms control and peace research scholars "…are not innocent pacifists convinced that good intentions are all that is necessary. Their work is highly scholarly and analytically powerfull with full understanding of the sociological and technological forces driving defense policies" .

When a novel research topic emerges, it is a common praxis for scholars and scientists to look at other disciplines for guidance, methods or simply fresh ideas to help them shed some light through the fog that normally envelops an "unknown territory". Computer scientists have looked at *biology* to explore new paths and develop more adaptable or self-healing computers (e.g. Kurtz et al. and Boneh, Dunworth and Lipton, no date given). Likewise examining biological warfare may provide useful hints about specific problems of information warfare (e.g. how to selectively target enemy's computers or how to circumscribe the virus' proliferation).

In the same manner, during the Cold War, indicators (proxies) helped security and peace research scholars (and intelligence services too) gain some knowledge about topics such as establishing the nuclear capabilities of superpowers that would have otherwise been completely out of their reach. For instance, Nye (2002: 26) recalls how indicators such as the number of scientists in nuclear R&D highly correlated with nuclear power status. Another example of the contribution of peace research scholars to the East-West debate during the Cold War is given by Risse-Kappen (1995). Risse-Kappen has explained how peace researchers and arms control scholars from both camps ultimately succeeded in creating international networks and hepistemic communities that were highly regarded in the West as well as in the East. Evangelista (1999) shares also the same conclusions.

One of the major changes from the conditions of the Cold War is that, without the Soviet Union, the United States has remained the world's only superpower. The United States is also the dominant player in information warfare. Consequently, that country is used, in this study, as the benchmark with which to determine the "CNO aptitude" of other countries. Information warfare analysts agree that Russia and China have also now invested considerable resources to develop CNO (Thomas, 2002a and

2002b). In addition to Russia and China, a handful of other countries are usually credited with CNO capabilities, namely France, the United Kingdom, and Israel and, perhaps, India and Pakistan (DoD, 2000). However, quoting unspecified CIA sources, figures as high as 100 countries have appeared on the media (Lettice, 2002).

Exploratory studies, like this work, can only elaborate tentative hypotheses. The hypothesis presented here asserts that since (a) only a handful of countries could effectively wage CNO and (b) with few exceptions, these countries are US allies or friends, digital wars, at least for the time being, are more a myth than a reality. If this hypothesis is proven true, then further investigation will be necessary to fully understand the reasons that have led to the creation and development of this myth.

Last, but not least, exploring the issue of CNO has considerable relevance for international and public affairs. As topics such as the Revolution in Military Affairs (RMA), Information Warfare (IW) or cyberterrorism enter the "public domain", opinion leaders, legislators and journalists, routinely (and, often, casually) use them. These terms have become "generic labels" for such a large number of possible occurrences to be, for all practical purposes, useless for researchers. Scholars should improve the research agenda on CNO to include more rigorous studies and thus contribute to reversing the hype and misinformation that now surrounds such important topic.

Despite the secrecy surrounding research and figures on CNO and the fact that after September 2001 several governments have curtailed online information, for all practical purposes, public sources can still provide scholars with useful data and valuable insights. Even before the “age of the Internet”, Dunnigan and Bay noted that “…censors would scream if they found out what a good library can provide” (1991: 630). Needless to say, this work is exclusively based on open source information.

The Status of Current Research and Relevance of The Topic

The end of the Cold War has created a whole new set of non-state actors that have adopted asymmetric forms of warfare to challenge established states. At the same time, the Revolution in Military Affairs (RMA) has multiplied "new warfare areas" (McKitrick et al., 1998). These combined effects are generally evident in the new realm of "Information Warfare/Information Operations" (IW/IO) and of Computer Networks Operations in particular.

Information warfare, which is the broader cathegory that includes CNO, has become one of the new post-Cold War era national security axioms, and a body of literature on the subject of CNO is now available.[4] With few exceptions[5], however, attempts at producing good "measurements" of still undefined concept have been scarce.[6] The experience of the Y2K bug is quite puzzling and of little practical help. Since no major disaster happened, technology skepticks argue that the problem was "blown out of proportion" and that the bug only helped software companies to sell their "patches". Those that expected modern societies would come to a standstill

[4] A brief summary of the most relevant publication in the field should include Alberts (1996a and 1996b), Aldrich (1996), Arquilla and Ronsfeld (1993, 1997 and 2001), Libicki (1995 and 1997), Campen, and Dearth (1998), Denning (1998). These books provide most of the theoretical framework for the debate on IW. Useful bibliographical references on the topic can be found at <http://www.au.af.mil/au/aul/bibs/infowar/if.htm> (by the US Air Force, update to 2002), <http://www3.cm.deakin.edu.au/~vstagg/infowar/biblio-ol.html> (by Infowar Australia, updated to 2002), <http://www.informatik.umu.se/~rwhit/IWBib.html> (by R. Withaker, updated to 1998) and <http://userpage.fu-berlin.de/~bendrath/IW-Literatur.html> (by R. Bendrath, updated to 1998 with several references to Europe and the Information Society). Sanz (1998) also provides an extensive bibliography.

[5] See for instance Rathmell (1998) and Gass and Romet (1998).

[6] I do not consider here classified reports by various intelligence agencies, which are not publicly available. A notable exception used to be the U.S. Department of Defense Military Critical Technologies List (MCTL) that included some evaluations of selected foreign countries (NATO and non-NATO). However, the 2000 edition of the MCTL currently available at <http://www.dtic.mil/mctl/> (*revised in 2002*) goes from pg.7 to pg.9, skipping pg.8. In an earlier printed version, on pg. 8 there was a "Worldwide Technology Assessment" providing information about evaluation of IW foreign capabilities (DoD 2000). Some data from that section have been included in the database as reference points.

claim that nothing happened precisely because those societies allocated resources and personnel to tackle the problem. With this precedent, it is unsurprising that considerable ambiguity surrounds the concept of CNO. While serious research on CNO is still in a very early stage, media reports continue to be based (for most part) on anedoctal evidence, rumors (e.g. Stone, 2001 and UPI, 2001), or theoretical speculation.[7]

The paradox of CNO is that computers and computer networks have led to major advances in economics, communications and war-fighting capabilities. But, at the same time, they have also made societies and economies as well as their related military forces more vulnerable to attacks on these networks. For modern societies, computer networks are truly "double-edged swords."[8]

For these reasons, some military professionals honestly admit that they are struggling to fit CNO in their organizational culture. In most countries, the main task of the military is to defend their government and the society they embody, but fulfilling this goal in cyberspace may appear like a overwhelming task. As Rattray (2001) correctly points out, to integrate new weapon systems in their operational plans and to develop a new doctrine for effective defense can take considerable time.[9] Moreover, in the military literature, defensive CNO (how to protect one's own

[7] The news article from UPI quotes a U.S. Air Force General, saying that "...North Korea, Iran, Iraq and other nations are working on cyber-attack capabilities that threaten the U.S. military's increasing reliance on information systems". However, it has been hard to find more detailed analysis on the actual cyberwar capabilities of those countries.

[8] "[O]n one edge representing areas that war-fighting components must protect, while on the other edge creating new opportunities that can be exploited against adversaries or used to promote common interests" (DoD, 1998: I-11).

[9] At the onset of World War II, Germany made exemplary use of platforms (i.e. tanks and airplanes) that had been developed in the second half of World War I, i.e. more than 30 years earlier. Eventually, all other major belligerents copied and improved (especially the Russians) German operational methods.

computer networks) attracts much more attention than offensive CNO,[10] perhaps in the attempt to downplay the latter.

Indeed, CNO have the *potential* to satisfy the crucial rule for military effectiveness that makes it different from analogous forms of warfare such as electronic warfare (EW). CNO are more than a simple, new complement to EW because it could actually fulfill the "break things and kill people" (BTKP) rule.[11] Since "...critical infrastructures are potentially vulnerable...because systems are complex..." (Denning, 2001), CNO seems to have the makings of a formidable weapon.

In this article, I have adopted a definition of CNO that is akin to the yardstick that professional soldiers everywhere use to judge the efficiency of war-fighting tools. First, I have focused on CNO waged against critical information infrastructures. The US Critical Infrastructure Assurance Office (CIAO) defines "critical infrastructures" as "[t]hose systems and assets—both physical and cyber—so vital to the Nation that their incapacity or destruction would have a debilitating impact on national security, national economic security, and/or national public health and safety."[12] The effects of

[10] An interesting exception seem to be the Chinese, who concentrate considerably to what IW could do to their enemy's communication and computer Networkss failing to appreciate what may happen to their own's (Yoshihara, 2001: 25).

[11] If CNO were valuable only to disrupt enemy's C4I systems (Command, Control, Communications and Computers, and Intelligence), it would only qualify as a new tool for EW, that is a force multiplier fpr other weapons that would cause the actual killing and estruction. But in the *most forceful case* (which is the one considered here), CNO could cause mechanical failures leading to loss of human lives or considerable economic damage. In these respects, CNO have the potentiality to "break things and kill people" the way that military planners would find appropriate. The BTKP rule sometimes receives truly "excessive" endorsing such as the statement of US Senator John Edwards who affirmed that: "We live in a world where a terrorist can do as much damage with *a keyboard and a modem as with a gun or a bomb*," (emphasis added). See the press release for the Cybersecurity Preparedness Act (January 2002) at http://edwards.senate.gov/press/2002/jan28-pr.html>.

[12] Originally (i.e. in the Presidential Decision Directive, PDD-63, of May 1998), the sectors identified as "critical" were eight, which have then reorganized into six areas (i.e., information and communications, electric power, transportation, oil & gas, banking & finance, water and emergency services) <http://www.ciao.gov/publicaffairs/about.html>. The concept and definition of critical infrastructures is evoked also in the USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) approved by US Congress on October 2001 as follows “systems and assets, whether physical or virtual, so vital to the United

material damage to these infrastructures would then entail loss of human lives or considerable economic damage or both.[13]

Second, to qualify as CNO,[14] such damage should be achieved by an attacker through either direct computer attacks (i.e. gaining unauthorized access to computers to take control) or other *digital* tools (i.e. viruses, worms etc.) whose injection in the system cause its malfunctioning and thus its failure. This definition of CNO implies that certain attributes that such as psychological operations (PSYOP), open source intelligence (OSINT), Web defacement and *hacktivism*, and, to some extent, cybercrime do not fulfill the BTKP rule and are thus marginal to this research.[15]

Critics may argue that the BTKP rule could lead to overlook other important features of CNO. That is, by achieving information superiority one could outsmart an adversary, or, thought more effective perception management (the old propaganda), may demoralize the other into apathy. In both instances, an opponent may obtain that victory without fighting that Chinese strategist Sun Tzu portrayed as superior to other forms of winning. The counterargument to this criticism is that in the history of warfare, winning without fighting like, for instance, Napoleon at Ulm (1805) is the exception, not the rule (widespread bloodshed is rather the norm). To impose one's will, one has to go through Clausewitz's friction, which, inevitably implies killing and destroying.

Thus far, the most efficient (and reasonable) applications of CNO appear to be (a) as a surrogate psychological "dirty" bomb, (b) as a direct attack against the world's

---

States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" (p.131).

[13] These are necessary specifics for a system to be defined as *critical*.

[14] Generally speaking, IW/IO may also imply the use of kinetic weapons, for instance, to take out some Internet nodes. CNO, on the other hand, would rely only on *digital* tools.

[15] For a list of themes that, normally, belong to the *broad* characterization of information warfare see the glossary in DoD (1998) and several of the contributions to Arquilla and Ronsfeld (2001).

financial/banking system and (c) as an ancillary tool in conjunction with other physical attacks (e.g. to block emergency services communications).[16] All these alternatives have advantages and disadvantages. In the scenario (a), CNO can magnify the psychological consequences of another event with strong emotional significance, helping to spread panic and confusion (the speed with which virus hoaxes spread is a good indicator of how effective this exploit would be). This use would be the fastest and most cost-effective application but also the most flimsy on the "break things and kill people" scale.

The (b) option is closely related to the previous one. Institutional investors and financial markets are extremely sensitive to any news that may have even some remote effects on the world economy. Hence, orchestrating a coordinated attack that, on the one hand spread false business information and, on the other, temporarily blocked (e.g. with simple denial-of-service) the communications to and from a few major banks or stock exchanges could seriously damage the economies of several advanced countries. Such attack would be on critical systems (as previously defined) and would have concrete and perhaps long-lasting consequences. In the scenario (c), an CNO attack would again have the role of "force multiplier", contributing to widen or prolong the effects of other physical actions such as bombs. A highly effective plan would probably combine (a), (b) and (c) together.

Such an act would probably be feasible and its consequences would be enormous and the economic losses gigantic. Nonetheless, (i) only state actors, thus far, have the resources of planning and executing such attack; (ii) if a state executed the attack some early intelligence would probably be available; (iii) it is hard to

[16] The latter are called “swarming attacks”. Apparently, the Networks Information Protection Center (NIPC) has published a paper on this topic but it is limited distribution (personal communication, November 13, 2002).

conceive how this attack would *not* have repercussions even on economy of the perpetrator state; (iv) the loss of human lives due only to the "cyber" segment of the attack (hence, discounting losses from explosions or chemicals) would be small.[17] Military planners and defense analysts are well aware of these intricacies (and that explains why skepticism has long pervaded the debate about the practicability of CNO as an efficient technique for war-fighting) but have not always been open in voicing their doubts.[18]

These conditions become, if possible, even more complicated if non state actors are involved. Potential cyberterrorists would have to operate from countries with reliable communication (not "remote" places like Afghanistan). They would have to hire highly trained personnel to do an effective job. They would also have to plan a physical attack to materialize *in coordination* with the cyberattack, if they aimed to fulfill the BTKP rule.

In examining the potential rise of cyberterrorism,[19] Denning (2001) reckons that for terrorists to regard strikes at computer networks as a viable weapon, " ...the attack should be sufficiently destructive or disruptive to generate fear comparable to that from physical acts of terrorism. Attacks that lead to death or bodily injury, extended power outages, plane crashes, water contamination, or major economic

[17] An "efficient" example of information warfare was the September 11th attack that, not counting human lives lost, almost blocked (and certainly slowed down) Internet traffic between Europe and the United States for almost two days (one of the backbone cable passed under the World Trade Center) and delivered a blow to financial markets, which, in turn, hasten the recession of American economy (see for instance Vatis, 2001: 12).

[18] On this point, see for instance Smith (1998) and the list of "cyberwar" that Vmyths.com regularly compiles (<http://vmyths.com/resource.cfm?id=23&page=1>.

[19] Although cyberterrorism is not central to this paper, it definitively fit in the class of "netwars" and thus it definitively relates to IW research. Moreover, because the availability of ready-to-use tools and the instinctive anti-government and anti-business postures of many hackers, many observers see cyberterrorism as one of the most likely forms of future infowars (e.g. Vatis, 2001 and Webster et al., 2001). However, as Denning rightly concludes, for the moment, cyberterrorism fails the BTKP test.

losses would be examples."[20] Denning concludes that, for the time being, more "traditional" forms of terrorist attacks (e.g. biological attacks or truck bombs) are more dangerous. News about alleged interest by al-Qaeda members in cyberattacks of the BTKP type have confirmed Denning's view (Anderson, 2002 and Gelleman, 2002).

Until recently, experts in the field of computer security have mostly agreed that, while there were some risks, the probability that, via computer networks, an external attacker could take command over or disable control nodes[21] of information infrastructures would be quite remote (Anderson, 2002 and Gellman, 2002).[22] Moreover, intelligence agencies concurred that only a few states would have the resources and technical skills to plan and execute such computer networks operations.[23] Although disagreement has increased among specialists about what

[20] This description is fully coherent with the military BTKP rule.

[21] Digital switches (called distributed control systems, or DCS) have almost completely replaced hardware parts in panels for process control that operate complex information or service distribution infrastructures. This change has several advantages: software is more easily upgraded, more scalable (i.e. more units can be added to the system) and cheaper than hardware counterparts. Moreover, maintenance personnel can remotely supervise (and even modify in real time) the software programs that control the functioning of these infrastructures. These software application programs belong to the category of "supervisory control and data acquisition" (SCADA) systems. SCADA are used in power plants as well as in oil and gas refining, telecommunications, transportation, and water and waste control , see < http://whatis.techtarget.com/definition/0,,sid9_gci555434,00.html>.

[22] Virusmyth.com has analyzed in details the "Australian case", that is the SCADA attack that received such wide media coverage) <http://vmyths.com/rant.cfm?id=458&page=4>. The "Australian case" involved a consultant (thus not an external intruder) for a water supply and wastewater management company that used his insider knowledge to compromise a public utility system so that he could secure a better-paide contract to solve the problem he had caused.

[23] The number of actual states with the capabilities to achieve these goals is highly controversial. Even relying on US intelligence sources, which are often the *only* ones available, figures considerably vary. Some publications mention the figure of *over* 20 countries with CNO capabilities (e.g. Vatis, 2001: 12 and Defense Science Board, 2001: 3), or, as mentioned earlier, even a hundred. The sources for these figures were not quoted, since, I presume, were classified. I tried to cross-check what countries may be included in that figure by looking at DoD Military Critical Technologies publication (2000), which analyze around 20 or 25 countries. The ranking of the DoD is consistent with the results of this research.

aggressors could achieve throughout on-line attacks because of the latest interests by terrorist organizations, these are more improbable events than conspicuous menaces.

In line with a "traditional" approach to exploratory research (e.g. Trochim, 1999:160 and King, Keohane and Verba, 1994), I have examined the literature now available on occurrences of "recognized" case studies of cyberattack activities (or netwars according to Arquilla and Ronsfeld, 2001). Table 1 below summarizes their findings and I have integrated it with other few cases emerged after the publication of Arquilla and Ronsfeld). "Type" indicates the kind of goal that the actors intended to pursue with the cyberattack.

Table 1 - Prominent Cases of Netwars 1994–2000

Campaign	Dates	Outcome	Type
Protracted Netwars			
Zapatista National Liberation Army	1994—	Limited success	Autonomist
ICBL (Landmines Campaign)	1998—	Limited success	Globalist
Burma	1996—	Failing?	Mixed
Drug Cartels	1994—	Substantial success	Autonomist
Chechnya I	1994–1996	Substantial success	Autonomist
Chechnya II	1999–2000	Failure	Autonomist
Israel/Palestine (Intifada)	2000-2001	Limited success	Autonomist
Short-Duration Netwars			
Greenpeace	1994	Limited success	Globalist
Battle of Seattle	1999	Substantial success	Globalist
East Timor	1999	Substantial success	Autonomist
Serbia/NATO (Kosovo Air War)	1999	Limited success	Mixed
Serb Opposition	2000	Substantial success	Mixed
China/United States (US Spy Plane Case)	2002	Limited success?	Mixed

(Source: Arquilla and Ronsfeld, 2001: 17)

Classification of some of these cases are problematic. Evidence from public sources has shown that some of the "virtual clashes" more closely resemble "netwars" than "cyberwars", but the distinction is never straightforward. For instance, after the incident with the U.S. spy plane of April 2002, quasi-national cyber war-fighting erupted between American and Chinese hackers against each other government's Web sites (the "Sino hackerwar"). The two governments were totally unconnected to the events. A similar state of affairs occurred in April 1999, when NATO planes mistakenly hit the Chinese embassy in Belgrade.[24]

Other scholars have used case studies of cyberattacks to support different options to defend from cyberattacks: from fostering country risk analysis techniques (Rathmell, 1998), to raise "cyber alert" (Vatis, 2001: 19), to increasing intelligence capabilities and adverting an "electronic Waterloo" (Webster et al. 2000). The crucial feature of most of these studies is that they rely on the analysis of cyberattacks such as Web defacement or Denial-of-Service (DoS) that are, by their nature, highly visible. While undoubtedly a nuisance and a financial loss in most instances, these acts can hardly be put to the BTKP test. A more sobering view of several instances of cyberattacks is provided by Vmyth.com, whose editors maintain updated list of "cyberwars".[25]

To conclude, those observers that claim that the cases mentioned above are actual threats and true instances of CNO not only fail to propose convincing yardsticks for measurement (such as, for instance, the BTKP rule) that would

[24] An excellent list on US/China and Israel/Palestinian "cyber-conflicts" is available under "Information Warfare" at Fred Cohen and Associates Web Site at <http://all.net/>. Apparently, the NATO/Serbia confrontation of 1999 over Kosovo witnessed also some instances of "cyberwar" (Wolf, 2001).

[25] The list is available at <http://vmyths.com/resource.cfm?id=23&page=1>.

persuade the intelligent reader of their findings. They also have contributed to turn the debate on CNO from a matter of serious research to a predominantly, media-oriented squabble.[26]

The Database: Operationalization and Possible Objections

The process of "operationalization" has followed the structure suggested in StatSoft (2002) and Trochim (1999). Public source military databases include scarce, if any, details on CNO, since governments prefer not to disclose actual figures on CNO capabilities.[27] Even assessments on electronic warfare capabilities are discontinuous, thus making it hard to proceed with cross national comparison. Inevitably, most of the data are proxies.

This section analyzes the operational concepts and the methodology used to create the data set. The data set is a cross-national comparison of 57 countries[28] that includes most of the advanced, industrialized economies, some newly industrialized (NIC) and a few less-developed countries (LDCs).[29] The availability of data entailed

[26] For instance, Vatis (2001: 12) quotes an article on Foreign Affairs by journalist James Adams as one of his sources for identifying those states with ambitious IW programs (Adams, 2001). Adams was the author of "The Next World War" that computer experts criticized for widespread inaccuracy when it was published (Smith, 1998).

[27] Figures on electronic warfare capabilities had not been collected coherently. The two main databases I surveyed were the *Military Balance 2001* published by the London-based International Institute for Strategic Studies (IISS) and Jane's Online *Armies of The World 2002* <http://online.janes.com/>.

[28] The data set originally contains 73 cases (countries). Since it was impossible to find all the data for all the 11 items selected for the scale, the actual scale ranks only 57 countries, i.e. those that had no missing values.

[29] Apparently, including LDCs in a study on infowar capabilities can be perceive by some observers as counterintuitive or puzzling. The reason for such an insertion of LDCs in this study is straightforward: several studies (e.g. Yoshihara, 2001and Shimeal, Williams and Dunlevy, 2001: 16) and, in general, the media (e.g. Havely, 2000 or Adams, 1998) have portrayed CNO as a sort of new "poor man's weapon of mass destruction". Gauthier (1999: 23) notes how some Chinese strategists have attempted to adapt Mao's concepts of people's war to IW, a sort of "every Chinese with a computer is a soldier". If this view of CNO becomes widely accepted (and several authors and experts on information warfare seem eager to do so, for instance Webster et al., 1998 but also, to some extents, Arquilla and Ronsfeld's concept of netwars), then it is crucial to include in a study like this some LDCs. In fact, these countries

that cases were selected using non-random sampling, which is a usual method in exploratory studies (see "Sampling" in Garson, 2002 and, more generally, Trochim, 1999 and Mugo, no date given). To some extents, the choice of this sampling technique restrict the resulting conclusions and generalizations, but international comparisons offer few if any alternatives.[30]

The logical process that has guided my selection of indicators is straightforward: lacking actual figures of CNO capabilities and access to classified data, I have devised a number of proxies that would provide a fair assessment of a country's CNO potential. The scale resulting from merging all these proxies would also offer a visual representation of where the different countries stand.

As already mentioned, analogous problems plagued arms control and peace research scholars during the Cold War. For instance, whereas estimations of conventional capabilities of NATO and the Warsaw Pact were quite unproblematic to formulate,[31] measuring nuclear (or chemical) arsenals was a harder job. Weapon systems such as tanks or artillery pieces are harder to "hide", while scientists develop nuclear weapons in *closed* laboratories (most research on CNO takes place in very closed labs). Nevertheless, scholars could look at civilian nuclear research programs (frequently available on public sources) to have a rough estimation of states' nuclear aptitude. Arms control students would add other details such as whether a countries had signed or not arms limitation treaties to sharpen their measuring.

(if one accepts the assumptions outlined above) should be the "ideal" supporters of CNO, since with relatively low budgets they can aim to wrecking havoc on a large economy's information infrastructure. At the same time, thye would be largely immune from any retaliation in kind, given their low dependability on computer Networkss. As a consequence of this reasoning, precision bombing of an enemy's information centers, despite how backward and archaic, is a key factor in part of information warfare for US military doctrine.

[30] For a discussion on the limits and common mistakes in using statistical methods see Clay Helberg, "Pitfalls of Data Analysis", Third International Applied Statistics in Industry Conference in Dallas, TX, June 5-7, 1995, <http://www.execpc.com/~helberg/pitfalls/>.

[31] On this point, see, for instance, Chalmers and Unterseher (1988).

I have followed the same pattern, collecting data on national technical competence, propensity toward high-tech and education levels in the relevant sectors. These data were then incorporated with other measures on computer security or communication infrastructures. The eleven proxies included in the scale can be divided into *three groups*:

(a) *general technical proficiency of the country* (export of high technology products, level of general education and relevant technical education);

(b) communication infrastructures and their use (number of Internet service providers, estimated Internet users and, as a single "infrastructure index", numbers of telephone lines and of *non secure*[32] servers);

(c) computer security and protection (number of CERT[33] teams, producers of encryption software and the number of *secure* servers) .

Within a certain degree of variation, these are the type of records that other databases appear to include (Gass and Romet, 1998, Rathmell, 1998, Schwartau, 1998 and DoD, 2000).[34]

---

[32] *Non* secure servers are computers that administer Networkss which require only low levels of security (e.g. a password and limited privileges for users) and do not handle sensitive information such as credit card numbers or individuals' health data. Only secure servers, which can routinely encrypt data and are protected by firewalls (i.e. computers that check the traffic between an internal Networks and the Internet), should handle such information.

[33] National Computer Emergency Response Teams (CERT) are groups of computer experts in private and public institutions (such as banks, universities or military installations) that monitor security breaches and then alert other similar parties so that similar incidents may be avoided.

[34] The DoD (2000)) list includes items such as intelligence systems, information security, software and high performance computing (fig.8.0-2, p.8-2) microelectronics and nanoelectronics (fig.8.0-1, p.III-8-3) or electronic attack and protection (fig.9.0-2, p.9-2). However, the available inventory of countries is quite limited (from five to 30). In their model for the database, Gass and Romet (1998) incorporate typologies such as encryption, software and Networks engineering, information security, malicious codes intelligence and communication (pp.354/55). Moreover, aware that obtaining precise figures for many such entries might be problematic, Gass and Romet (p.352) ingeniously suggest that the model should allow for fuzzy ratings, i.e. numerical values based on fuzzy logic (for an in-depth study of how fuzzy logic can contribute to social science research see Ragin, 2000). However, no specific data-set is provided. Rathmell (1998) builds on Gass and Romet's model and methodology (fuzzy ratings) and stresses the relevance of detailed case studies to construct "threat indices" (p.302). Rathmell's goal, however, is that of refining threat assessment and risk analysis methods for forecasting cyberattacks more than comparing state's potential (Rathmell indeed include non-state actors in his analysis). Finally, Schwartau (1998) offers a scheme of "cyber health" or "cyber-conditions" (like "defense

Another necessary qualification for this study is the explanation of why this research and my database do not consider states' intentions to undertake computer networks operations but only their capabilities. Given the importance of information infrastructures for the social and economic well-being of countries, researchers and scholars have devoted attention at forecasting and finding methods to assess intentions of foreign governments (Gass and Romet, 1998 and Rathmell, 1998). Techniques adopted to this goal are mostly akin to country-risk analysis methods (Wenger, Metzger and Dunn, 2002).

Generally speaking, evaluating states' intentions[35] is more the task of intelligence services than academic research, which should concentrate on testing theories or generating new hypotheses. Moreover, studying intentions and patterns of behavior of foreign governments to hedge against "bad" surprises is mostly a waste of time and resources. A surprise attack, whether with cyber or conventional or chemical/biological weapons, is most likely to succeed and it is not only a matter of how efficient an intelligence service is. As Betts (1982) convincingly argues, it is mostly political leaders that fail because they fall prey of their own political disbelief. These argumentation have convinced me to leave indicators for states' intentions out of the database.

The last clarification should be about the units of analysis chosen for this research. Since I am interested in cross-national comparison, the units are "sovereign states". First, if a cyberattack is carried through by a government's employees (i.e. the

---

conditions", with five levels) to evaluate the responsiveness of American business and the country as a whole (p.59). Schwartau does not provide data either and his model for a database is overly heuristic. I have repeatedly (and unsuccessfully) tried to acquire more information about the details and contents of these databases.

[35] In this context, forecasting means assigning probability that a foreign government intends, possibly with a certain degree of surprise, to use IW to strike one's own national information infrastructure.

army) or by a state sponsored group, according to international law, it qualifies as a true "act of war". Second, for the time being, only states are most likely to posses the necessary capabilities to wage effective CNO. When it comes to “threatening the digital world”, Schneier (2000: 54) rightly infers that government agencies are “the most formidable adversary around”. Finally, the process of developing operational categories for non state groups, which lately have acquired leverage and importance in international affairs and security, is still in its infancy. At this stage, including the latter in this data set would be exceedingly problematic.

The Database: Assessing and Ranking CNO Capabilities

Table 1 displays the ranking of the first 20 countries. As mentioned earlier, the United States is the "yardstick" with which to measure CNO capabilities of other countries. The findings confirmed the expectations, that is, the top 20 countries are either formal allies or, at least, have very friendly relations with each other.[36]

Table 1: The CNO War Index

Countries	CNOWar Index	Rank
UNITED STATES	0.86	1
AUSTRALIA	0.48	2
FINLAND	0.46	3
UNITED KINGDOM	0.45	4
SWEDEN	0.44	5
CANADA	0.43	6
NORWAY	0.41	7
NETHERLANDS	0.40	8
DENMARK	0.40	8
GERMANY	0.39	9
KOREA ROK	0.38	10
SWITZERLAND	0.37	11
IRELAND	0.37	11

[36] The full tableand the method to calculate the index are included in Appendix C. The entire data set (in Excel format) will be made publicly available when the article is published.

SINGAPORE	0.37	11
JAPAN	0.36	14
FRANCE	0.36	14
NEW ZEALAND	0.35	16
AUSTRIA	0.34	17
ICELAND	0.33	18
SPAIN	0.32	19
ITALY	0.31	20

Of the countries that many observers in the United States consider possible direct competitors (or worse), Russia is n.20, and China n.43, while India and Pakistan rank 53 and 57.[37] A comparison with other studies may also contribute to shed some light on this matter. For instance Table 2 shows the breakdown of cyber attacks by country of origins prepared by Riptech Inc. for the first semester of 2002.

Table 2: Comparison Between Attacks and Ranking on the CNO Index

Country	Percentage of Total Attacks	Relative Ranking on the CNO Index
United States	40.0	1
Germany	7.6	9
Korea ROK	7.4	10
China	6.9	43
France	5.2	14
Canada	3.0	6
Italy	2.7	20
Taiwan	2.4	/
Great Britain	2.1	4
Japan	2.1	14
Total	79.6	

(Source: Riptech, Inc. 2002: 29, Fig.25)

The major incongruities with Table 1 are (a) the position of China that ranks considerably higher here and (b) some countries show a different succession (e.g. Italy has a higher score than Great Britain and Japan or France comes before

Canada).[38] For the rest, Table 2 is fairly consistent with Table 1.[39] The DoD's Foreign Technology Assessment (FTA) for 2000, summarized in Table 3 provides another interesting piece for comparison.

Table 3: US DoD CNO Index (Unofficial)

COUNTRIES	DOD Est. Capabilities	DOD Index	DOD Ranking
UNITED STATES	40	1	1
UNITED KINGDOM	36	0.90	2
JAPAN	35	0.87	3
FRANCE	33	0.82	4
GERMANY	33	0.82	4
CANADA	28	0.69	6
ISRAEL	22	0.54	7
AUSTRALIA	21	0.51	8
NETHERLANDS	21	0.51	8
ITALY	20	0.49	10
RUSSIA	19	0.46	11
SWEDEN	19	0.46	11
NORWAY	16	0.38	13
SWITZERLAND	16	0.38	13
TAIWAN	14	0.33	15
CHINA	13	0.31	16
SPAIN	13	0.31	16
BELGIUM	12	0.28	18
BRAZIL	12	0.28	18
FINLAND	12	0.28	18
INDIA	10	0.23	21
DENMARK	9	0.21	22
SOUTH AFRICA	9	0.21	22
KOREA ROK	5	0.10	24
CZECH REP.	2	0.03	25
HUNGARY	1	0.00	26
TURKEY	1	0.00	26

(Source: US DoD, 2000: 8-2, Fig.8.0-2)[40]

---

[37] A possible incongruity in the data set is the position of Israel, n. 28.

[38] Taiwan was not computed to missing data for some of the items of the scale.

[39] According to RipTech (2002: 30, Fig. 26 and 27), conditions change considerably, however, when the ratio between the rate of attacks and number of Internet users is calculated. Israel and Hong Kong lead the list of "active" countries with more than one million users while Kuwait and Iran lead that with more than 100,000 users. Germany, France, South Korea and China appear in the former list, but not other countries such as the United States. Two points are worth considering here: (a) with the exception of Israel and China (Hong Kong was not calculated) that appear only in the mid and lower part of the CNO Index summary table (appendix C), Germany, France, and South Korea are present in the top ten list, thus showing consistency of the two studies; (b) the top position by Kuwait in the Riptech study can probably be explained by the fact that several host computers in that country are taken over by outsiders attackers that then use them to stage attacks elsewhere.

Once again, the same countries are present, albeit with different positions. The leading position of the United States justifies the decision to take that country as the "yardstick" with which to evaluate the CNO assets of other countries. The discrepancy that is most intriguing between Tab.1 and Tab.3 is the scope of the United States' lead over even the group of top countries. In the DoD Index the second highest ranking country, i.e. the United Kingdom scores .90 (the United States being 1). In the CNO Index, Australia, the second highest scoring country, hits only .48, far below the .86 of the United States. The graph (Fig.1) below from Tab.1 reveals more clearly the actual gap between the United States and the followers.

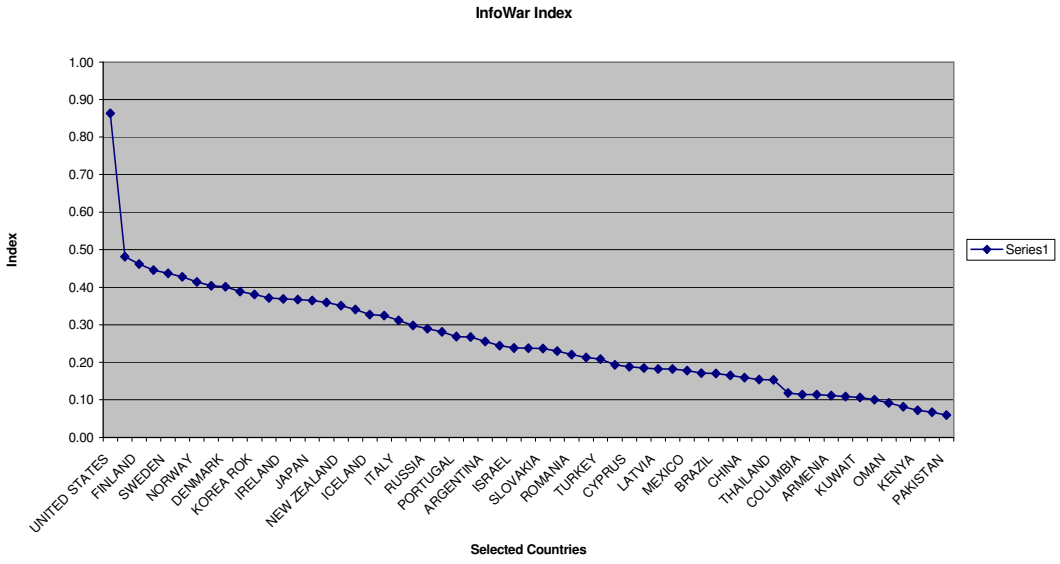

Fig.1

[40] For the FTA the DoD presents a scale of Critical Technologies Capabilities (CTC) ranging from four (full capabilities) to one (little capabilities) for 11 items. I selected ten of them and, on that basis and the available figures, created the index used in Table 3. The DoD does not provide details about the assessment of CTC.

Reliability and Validity

Reliability and validity are two crucial notions for research. They confirm that a study correctly and consistently measures the intended object of observation. Scholars employ various techniques are to achieve reliability and validity (e.g. Sullivan and Feldman, 1979, Carmines and Zeller, 1979, Trochim, 1999 and 2000).

The most common index to measure the reliability of a scale such as the one generated by this study is Cronbach's alpha and benchmarks may vary from .60 to .70/.80 (Sullivan and Feldman, 1979, Carmines and Zeller, 1979, Trochim, 1999 and 2000, StatSoft, 2002 and Garson, 2002). Alpha measure for the scale was .8322,[41] thus crossing the threshold for reliable scales.

Validity of a scale is less straightforward to evaluate than reliability. Items for the scale satisfy face and content validity ("do these items make sense in this scale?"). Construct validity (which is the most important form of validity) is somehow satisfied. The method applied in this research was akin to multi-method, multi-trait (MMTM) strategies, which are the most robust method to assess validity. These strategies imply that the researcher "...uses multiple indicators per concept, but also gathers data for each indicator by multiple methods and/or from multiple sources" (see "Validity" in Garson, 2002).

As mentioned above, using proxies instead of actual measurement may decrease overall validity. Nonetheless, all the selected items appear to capture some aspects of CNO. Furthermore, they correlate with each other acceptably (see appendix B) and Cronbach's alpha ("no reliability, no validity") is quite high. Under these

[41] Standardized item alpha (which is sometimes used instead of simple alpha) was .8831.

circumstances, it is possible to confirm that the criteria for validation are met and thus that the scale is reasonably both reliable and valid.

Conclusions and Prospects for Future Research

This paper has addressed two main questions: (a) are CNO a real contingency and (b) can CNO be measured? The definition adopted here of what should constitute actual computer networks operations rests on the "break things, kill people" rule. According to this definition, the only possible answer to question (a) is that computer networks operations—as defined in this paper—are mostly an exaggeration. An external attacker would have to be highly skilled and trained and be backed by considerable technical resources to access and take control or disrupt the key nodes of a national information infrastructure. It is no surprise that insiders, like disgruntled employees, are often the perpetrators of substantial destructive attacks (e.g. Verton, 2001). The classification of countries according to their CNO resources also shows that some form of approximate measurement is possible.

The scale of countries with CNO capabilities based on my data-set clearly show that, in addition to the United States, only a handful of countries should potentially be able of "waging" CNO. These countries are certainly more vulnerable than others that are less dependable on information infrastructure and computer networks. Yet, they also have the capacity to undertake effective computer networks operations. Given their digital prowess and military might, it is no surprise that these countries stand out. They epitomize a sort of the "usual suspects' club" of CNO. One may wonder, at this point, what is the originality of these findings. The novelty of these findings is precisely that there is no novelty, because these findings were expected. These countries are simply the main players in international affairs, world

economics and global security, *including* cyber security and they dominate computer networks and telecom. They should not fear any competitors.

Most notably, with the exceptions of China and Russia,[42] these countries meet the criteria of being current U.S. *allies* (e.g., Germany, France, and the United Kingdom) or *friends* (Israel or Canada) and have close political and economic ties with one another. Presumably, these countries should pose *no threat* to each other, whether on cyber or physical space. Hence, one should conclude that, with these relatively few exceptions, for many states (no matter their overall offensive or defensive predisposition) CNO are simply an option that belongs more to the realm of myth than that of reality.

If one accepts these facts and that it is unlikely that, at state level, new competitors will soon emerge from outside this group of countries, then research on CNO begins to move into more a complex but, at the same time, more interesting stage. The third question I posed at the beginning then surfaces again: "why did the question about the true 'nature' of CNO (myth or reality), in the first place, emerge?" Moreover, if, under the assumptions of this article, infowars are mostly a myth, "why, then, do they seem to represent an important catchword for some governments?"

Claiming full explanatory power for hypotheses formulated at this stage of the research would be rather foolish; yet, probing for new hypotheses is exactly the scope exploratory study such as this. As Kaldor (2001) has noted, to answer that question, perhaps scholars should start peering *inside* the governments of that group of main players and, more specifically, inside the United States' government.

With the end of the Cold War and after the Gulf War, the US Department of Defense and the whole national security community in the United States have looked

for a new institutional role. New analytical approaches to military thinking (the RMA), new weapon systems (e.g. unmanned vehicles with "smart" ammunitions) and new doctrines (e.g. operations other than war) were being prepared or polished. These tools would be ready-to-use, once that search were over. What was missing was *the* catalyst, such as the 1915 Lusitania, the first nuclear device exploded by the Soviet Union, or the Korean War that would persuade the American public that that new role was unquestionably necessary. Kaldor (2001) claims that September 11th provided that missing piece.

Before September 2001, information wars (in the "extended form", that is, including psychological operations, Web defacement, *hacktivism*, cybercrime, etc.) had been extremely functional in this search for new threats by various security communities. During the 1990s, in a sort of supply-driven process, intelligence and law enforcement agencies, government officials and national security personnel consistently appeared to compete with each other in offering a menacing picture of "cyberspace", in the attempt to persuade the American public that their services were indispensable.

Since, even sophisticated users in advanced societies have only a modest understanding of the operation of computer networks, at times, the American public opinion (and, consequently, Canadians, Europeans, Japanese and others) tended to accept those statements. Informed individuals, as well as the computer and telecom industries, remained nonetheless skeptical. Inevitably, what happened in September

[42] In the field of international security, China and Russia always come forward as possible U.S. opponents. Actually, more often than not, Russia now qualifies as a "friend" of the United States.

2001 has profoundly transformed the parameters of the security discourse in the United States and other democracies around the world.[43]

One of the major innovations of the post September 2001 security discourse was to shift the focus of national security in the United States (and among other US allies) from state to *non state* actors. Attention to cyber threats of non state origins such cybercrime and cyberterrorism predictably increased as well. Thus, objections to relying on data sets such at this that focus exclusively on states' capabilities to estimate the probability that some agent (state or non state) may exploit CNO as security tools to shape world politics are to be expected. Moreover, should the current trend of modern society of moving toward an "embedded computing" environment[44] continue, the opportunities for technological destruction would considerably increase.

There are certainly overlapping aspects between cybercrime and cyberterrorism.[45] Perhaps, as more non state groups learn to appreciate the advantages of some of the techniques of computer networks operations, the demand for CNO readiness and cyber threats will become more compelling. The "computerization" of societies and economies is unlikely to stop. Nevertheless, for the time being, the logic of this argument is plain wrong.

First, as this work has shown, several of much quoted cases of cyberattacks have, thus far, failed to meet the BTKP rule. Instead of advancing serious scholarship, some studies (e.g. Adams, 2001) have actually contributed to the media frenzy and the imprecision and confusion that inevitably derives from such state of affairs.

---

[43] Focusing on information warfare, Bendrath (forthcoming) provides and excellent analysis of the changing of the security discourse in the United States during the Clinton, pre and post 9/11 Bush Administrations.

[44] In an "embedded computing" environment, computing power instead of being embodied in personal computers or maunframes is simply integrated in all electronic devices that are all networked and communicate with each other.

Second, "embedded computing" environments may prove to be more resilent than the current model because it should stress redundancy that is one of the elements that computer and security experts alike consider important for systems to survive attacks.

Third, given these precedents, even if cyberterrorism is considered to be a form of CNO, it will take even longer for the former to fulfill the BTKP rule. Terrorists groups will have to either hire skilled technicians or train their own computer experts. These solutions are both expensive and take long time to implement. More importantly, the decision to embrace cyberterrorism will imply considerable adaptation of the organizational culture of terrorist groups.

Finally, as Denning (2001) noted, for the time being, other forms of asymmetric warfare such as bioterrrosim or car bombs will remain the likely instruments of non state groups challenging sovereign states. For these reasons, studying the capabilities of non state actor and included them in a data set such as this may acceptably remain on the *long term* agenda of this research.

This article has followed the critical approach of arms control and peace research scholarship that came of age during the Cold War. It took arms control and peace research scholars considerable time to set up extensive, and reliable databases—which other researchers have then used to test new hypotheses or challenge established theories—but the final results of those efforts paid off remarkably.[46]

---

[45] For instance, organizations operating in both areas rely on Networksing structures and dispersed, communication systems. Organized crime is also likely to adopt some of the Networksing features of modern terrorist organizations.

[46] The FIRST (Facts on International Relations and Security Trends) database by SIPRI-ISN (Stockholm International Peace Research Institute and the International Security Networks) and other institutions is available on-line at <http://first.sipri.org/>. The database contains "...hard facts on armed conflicts and peace keeping, arms production and chronology, statistics and other reference data". For a discussion on the methodology used to collect data for these databases see Hagmeyer-Gaverus, (1998) and Isenberg, (1998).

This article is just an early step in a long process of refining definitions, typologies and measurements of infowars. It is a much exploratory undertaking, thus far from yielding definitive results. More comprehensive data sets are necessary. Arms control and peace research scholars should collect large amount of *qualitative* information to be analyzed, put into numerical format (as ordinal variables or, alternatively, as fuzzy-sets) and added to indexes such as the one presented here.

In all likelihood, public sources (as those used for this article) on military CNO programs and CNO-war-fighting agencies will remain the only option for most scholars. Ultimately, these circumstances will guarantee better transparency of the data used for future analyses, as well as greater public accountability of the researchers involved in this endeavor.

In an era that combines RMA, asymmetric forms of warfare and increasing reliance on information infrastructures, cooperative outcomes such as innovative arms control treaties are possible only if reliable information is made available to the wider community of scholars, practitioners and the informed public. No serious academic and public debates can take place without open access to more dependable literature, or until more studies, based on competing methodologies, are produced. Once these debates begin, however, they inevitably have spill-over effects in the political arena and have a great potentiality to influence the policy-making process.

At the onset of the Cold War, the task of providing reliable data on conventional forces or nuclear, chemical and biological (NBC) warfare must have appeared mostly intimidating to those independent researchers who did not have access to classified information. Those scholars were also well aware that, in many instances, their work would be the main reference point for debates on disarmament and arms control for some of the actors involved in those debates, such as peace

movements or opposition parties. The range and proficiency of studies on conventional and NBC warfare that have appeared since, it is an unquestioned tribute to the insight and determination of those scholars. Independent research on CNO is now in the same situation as arms control and peace research was at the onset of the Cold War. Will it ultimately match the quality and insight of its predecessors?

SELECTED BIBLIOGRAPHY

Adams, James. 1998. *The Next World War: Computers Are the Weapons and the Front Line Is Everywhere*. New York: Simon & Schuster.

——. 2001. Virtual Defense. *Foreign Affairs*. May/June. 98-112.

Alberts, David S. 1996a. *The Unintended Consequences of Information Age Technologies*. Washington, DC: National Defense University.

——. 1996b. *Defensive Information Warfare*. Washington, DC: National Defense University.

Aldrich, Richard 1996. The International Legal Implications of Information Warfare. *INSS Occasional Paper* 9 in the Information Warfare Series, Colorado Springs CO: US Air Force Academy's USAF Institute for National Security Studies, <http://www.usafa.af.mil/inss/ocp9.htm>.

Anderson, Kevin. 2002. " US 'fears al-Qaeda hack-attack' ", *BBC NEWS Online* June 27, <http://news.bbc.co.uk/1/hi/sci/tech/2070706.stm>.

Arquilla, John and David Ronfeldt, eds., 2001. *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica: RAND MR-1382-OSD.

—— eds. 1997. *In Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica: RAND MR-880-OSD/RC.

——. 1993. Cyberwar is Coming! *Comparative Strategy*. 12: 141-165.

BBC News On Line (2001), "Truce' in US-China Hacking War", May 10, <http://news.bbc.co.uk/hi/english/world/asia-pacific/newsid_1322000/1322839.stm>.

Bendrath, Ralf. The American Cyber-Angst and the Real World – Any Link? In *Bytes, Bombs, and Bandwidth*, edited by R. Latham, New York: New Press, (forthcoming).

Betts, R.ichard, K. 1982. *Surprise Attack: Lessons for Defense Planning*. Washington, D.C.: Brookings Institution.

Boneh, Dan, Cristopher Dunworth and Richard J. Lipton. Date not given. Breaking DES using a molecular computer. Princeton University, <http://crypto.stanford.edu/~dabo/papers/bioDES.ps.gz>.

Campen, Alan D. and Douglas H. Dearth, eds., 1998. *Cyberwar 2.0*. Fairfax, VA: AFCEA International Press.

Campen, Alan D. 1992. *The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War*. Fairfax, VA: AFCEA International Press.

Carmines Ernest and Richard Zeller. 1979. *Reliability and Validity Assessment*. Newbury Park and London: Sage University Press.

Chalmers, Malcom and Lunz Unterseher. 1988. Is There a Tank Gap? Counting NATO and Warsaw Pact Tank Fleets. *International Security*. 13: 5-49.

Critical Infrastructure Assurance Office (CIAO). 2000. National Plan for Information Systems Protection, Version 1.0. The White House, <http://www.ciao.gov/publicaffairs/np1final.pdf>.

Denning, Dorothy. 2001. Is Cyber Terror Next? In *Understanding September 11* edited by C. Calhoun, P. Price, and A. Timmer, PP, New York: The New Press (also at <http://www.ssrc.org/sept11/essays/denning.htm>).

——. 1998. *Information Warfare and Security*. Boston, MA: Addison-Wesley.

Department of Defense (DoD). 2000. Military Critical Technologies, Part III: Developing Critical Technologies, Section 10: Information Technology. Dulles, VA: Defense Threat Reduction Agency, May < http://www.dtic.mil/mctl/>.

——. 1998. Joint Doctrine for Information Operations. October 9. <http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf>.

Dunnigan, James F. and Austin Bay. 1991. *A quick and dirty guide to war. Briefings on present and potential wars*. Revised Edition. New York: Quill William Morrow.

Evangelista, Matthew. 1999.*Unarmed forces: The transnational movement to end the Cold War*. Ithaca: Cornell University Press.

Garson, David, 2002. *PA 765 Statnotes: An Online Textbook*, <http://www2.chass.ncsu.edu/garson/pa765/statnote.htm>.

Gass, N. and T. T. Romet. 1998. A Framework for Modeling the Threat of Information Operations and the Infrastructure of a Country. In *Cyberwar 2.0* edited by A. Campen, and D. Dearth Fairfax, 347-358. VA: AFCEA International Press.

Gauthier, Kathryn L. 1999. China as Peer Competitor? Trends in Nuclear Weapons, Space and Information Warfare. Air War College Paper No.18, Maxwell Air Force Base, AL.

Gellman, Barton. 2002. Cyber-Attacks by Al Qaeda Feared. *The Washington Post*, June 27, p.A01

Gerring, John. 2001. *Social Science Methodology: A Criterial Framework*, Cambridge: Cambridge University Press.

Green, Thomas C. 2000. "Cyberwar in the Middle East". *The Register*, October 27, <http://www.theregister.co.uk/content/archive/14295.html>.

Hagmeyer-Gaverus, Gerd. 1998. Information Needs and Database Use in the Field of International Relations and Security. Stockholm International Peace Research Institute <http://www.sipri.se/projects/database/infosystem/databases.pdf>.

Havenly, John. 2000. When States Go to Cyber-War. *BBC News On Line*. February 16, <http://news.bbc.co.uk/hi/english/sci/tech/newsid_642000/642867.stm>.

Hersman, Tania. 2001. Israel Discusses the 'Inter-fada'. *Wired News*. January 12, <http://www.wired.com/news/politics/0,1283,41154,00.html>.

Hoffman, Lawrence. et al. 1999. Growing Development of Foreign Encryption Products in the Face of U. S. Export Regulations. Report GWU-CPI-1999-02. Washington, DC: Cyberspace Policy Institute, George Washington University, <http://www.cpi.seas.gwu.edu//library/docs/cpi-1999-02.pdf>.

Horn, Robert V. 1993. *Statistical Indicators for the Economic and Social Sciences*. Cambridge: Cambridge University Press.

Kaldor, Mary. 2001. Beyond Militarism, Arms Races and Arms Control. In *Understanding September 11* edited by C. Calhoun, P. Price, and A. Timmer, PP, New York: The New Press (also at <http://www.ssrc.org/sept11/essays/kaldor.htm>).

King, Gary, Robert O. Keohane and Sidney Verba. 1994. *Designing Social Inquiry: Scientific Inference in Qualitative Research*. Princeton: Princeton University Press.

Kurtz, Stuart et al. Date not given. Biological Computers. University of Chicago, <www.cs.uchicago.edu/~stuart/Research/MRSC.pdf>.

Isenberg, David. 1998. Computer: Access the Arms Sales Database. Internet Information: Doing Better with What We Have. Stockholm International Peace Research Institute (SIPRI), <http://www.sipri.se/workshop/Isenberg.pdf>.

Lettice, John,. 2002. At least 100 countries building cyber weapons – expert. *The Register*. September 24, <http://www.theregister.co.uk/content/6/27265.html>.

Libicki Martin. 1995. What Is Information Warfare. *ACIS Paper* 3. Washington, DC: National Defense University.

——. (1997), *Defending Cyberspace*, Washington, DC: National Defense University.

McKitrick, John. et al. 1998. The Revolution in Military Affairs. In *Battlefield of the Future: 21st Century Warfare Issues*. Aerospace Power Chronicles, <http://www.airpower.maxwell.af.mil/airchronicles/battle/bftoc.html>.

Mugo, F.W. No date given. Sampling in Research. In *Research Methods Tutorials*, <http://trochim.human.cornell.edu/tutorial/mugo/tutorial.htm>.

Nye, Joseph. 2002. *The American Paradox: Why the World's Only Superpower Cannot Got It Alone*. Oxford: Oxford University Press.

Ragin, Charles. 2000. *Fuzzy-set social science*. Chicago: University of Chicago Press.

Rathmell, Andrew. 1998. Assessing the IW Threat from Sub-state Groups. In *Cyberwar 2.0*, edited by A. Campen, and D. Dearth, 295-312. Fairfax, VA: AFCEA International Press.

Rattray, Gregory. 2001. *Strategic Warfare in Cyberspace*. Cambridge, MA: MIT Press.

Riptech. 2002. Internet Security Threat Report. January. Alexandria, VA.

Risse-Kappen, Thomas. 1995. Ideas do not float freely: Transnational coalition, domestic structure and the end of the Cold War. In *International relations theory and the end of the Cold War*, edited by R. Ned Lebow and T. Risse-Kappen, 187-222. New York: Columbia University Press.

Robertson, David. 1987. *A dictionary of modern defence and strategy*. London: Europa Publications Inc.

Russett, Bruce M. et al. 1977. *World Handbook of Political and Social Indicators*. Westport: Greenwood Press

Sanz, Timothy L. 1998. Information-Age warfare: A Working Bibliography, Part II. *Military Review*. 78 National Defense University Library, <http://merln2.ndu.edu/wget/www-cgsc.army.mil/milrev/English/SepNov98/PDF/sanz.pdf>

Schneier, Bruce. 2000. *Secrets and lies: Digital security in a Networked world*. New York: Wiley and Sons.

Schwartau, Winn. 1998. Something Other Than War. In *Cyberwar 2.0*, edited by A. Campen, and D. Dearth, Fairfax, 55-63. VA: AFCEA International Press.

Shimeall, Timothy, Phil Williams and Casey Dunlevy. 2001/2002. Countering Cyber War. *NATO Review*. Winter.16-18.

Smith, George. 1998a. An Electronic Pearl Harbor? Not Likely. *Issues on Science and Technology Online*. Fall, <http://205.130.85.236/issues/15.1/smith.htm>.

——. 1998b. Truth Is the First Casualty of Cyberwar. *Wall Street Journal On Line* September 8, <http://www.soci.niu.edu/~crypt/other/wsj.htm.

StatSoft Inc. 2002. Reliability and Item Analysis. In *Electronic Statistics Textbook*. Tulsa, OK: StatSoft < http://www.statsoft.com/textbook/stathome.html>.

Stone, Janet A. 2001. Cyberspace: The Next Battlefield. *USA Today On line*. June 19. In Infowar: Military and C4I <http://www.infowar.com/ >.

Sullivan John L. and Stanley Feldman. 1979. *Multiple indicators: An introduction*. Beverly Hills and London: Sage University Press

Taylor, Charles L. 1972. *World Handbook of Political and Social Indicators*. New Haven: Yale U Press .

Trochim, William. 1999. *The Research Methods Knowledge Base*, 2nd ed., Itacha, NY: Cornell University Custom Publishing, <http://trochim.human.cornell.edu/kb/index.htm>.

United Nations Development Program (UNDP). 2001. *Human Development Report: Making New Technologies Work for Human Development*. Oxford and New York: Oxford University Press, <http://hdr.undp.org/reports/global/2001/en/default.cfm>.

United Press International (UPI). 2001. Military Fears Attacks From Cyberspace. April 3. In Infowar: Military and C4I, <http://www.infowar.com/ >.

United States Congress. 2001. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT), Public Law 107–56—Oct. 26
<http://www.cdt.org/security/usapatriot/011026usa-patriot.pdf>.

Vatis, Micheal. 2001. Cyber Attacks During the War on Terrorism: A Predictive Analysis. Institute for Security Technology Studies, Dartmouth College, September 22
<http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_a1.pdf>.

Verton, Dan. 2001. Analysis: Insiders a major security threat. *CNN Online*. July 11.
<http://www.cnn.com/2001/TECH/industry/07/11/insider.threat.idg/>.

Yoshihara, Toshi. 2001. Chinese Information Warfare: A Phantom Menace or Emerging Threat*?* Harvard University Program in Information Resources Policy,
<http://pirp.harvard.edu/pubs_pdf/yoshiha\yoshiha-i01-3.pdf>.

Webster, William. et al. 1998. Cybercrime...Cyberterrorism...Cyberwarfare: Adverting an Electronic Waterlo*o*. Washington, DC: Center for Strategic and International Studies (CSIS) Global Organized Crime Project.

Wenger, Andreas, Jan Metzger and Myriam Dunn, eds. 2002. Critical information infrastructure handbook: An inventory of protection policies in eight countries. Center for Security Studies and Conflict Research, Swiss Federal Institute of Technology, Zurich, Switzerland.

Wolf, Jim. 2001. U.S. Prepares for Cyberwar—the War Next Time. In Infowar: Military and C4I, November 8, <http://www.infowar.com/ >.

APPENDIX A
THE CODEBOOK
(Detailed Methodology and Selection of Data and Indicators)

Indicators and Sources for Data

This Appendix contains (a) explanations about the choice of indicators; (b) sources of these indicators; (c) how the indexes were created, and (d) the statistical methods applied. The same points were mentioned briefly in the main text and this Appendix is intended to expand on those point for further clarification.

1. ***CERT Teams*** (also CERT)* (X1) CERT (Computer Emergency Reaction Teams) teams are groups of computer security experts that respond to threats such as viruses or intrusions. These teams are created/hosted by private (i.e. banks or telephone companies) or public (governments or universities) actors. Most CERTs belong to an international association, the FIRST (Forum of Incident Responses and Security teams.
   Source: FIRST Web sites, <http://www.first.org/team-info/> for the period 1999/2002.

2. ***High Tech Trade*** (also TCHTRADE) (X2) is the high-technology export (as percentage of manufactured export) in the sample countries. Data are for 1999.
   Source: UNDP Human Development Report 2001
   <http://hdr.undp.org/reports/global/2001/en/indicator/indicator.cfm?File=list_indicators.ht>

3. ***Net User Estmd*** (also ESTUSER) (X3) is the estimated number of Internet users. Data are for 2000. Source: CIA World Fact Handbook, 2001
   <http://www.cia.gov/cia/publications/factbook/>

4. ***Encrypt Softwr*** (also ENCRYPT) (X4) is the number of encryption software producers.
   Source: Hoffman et al. (1999) <http://www.cpi.seas.gwu.edu//library/docs/cpi-1999-02.pdf> for all countries but the United States. For the *United States*, Networks Associates, Cryptographic Technologies (as of June 30, 2001)
   <http://www.nai.com/research/nailabs/cryptographic.asp>

5. ***Tech Skills*** (also TECSKL) (X5) is the number of students enrolled in tertiary education in science and engineering disciplines (as percentage of the population of the relevant age group). Data are from 1995/1997.
   Source: UNDP Human Development Report 2001
   <http://hdr.undp.org/reports/global/2001/en/indicator/indicator.cfm?File=list_indicators.html>

* The different notation is due to restrictions package used for this research (SPSS) put on the length on the variable name that the statistical (eight characters).

6. ***ISP*** (also ISP) (X6) is the figure of Internet Service Providers (ISP) in a given country.
   Source: CIA World Fact Handbook, 2001
   <http://www.cia.gov/cia/publications/factbook/>

7. ***Educ*** (also EDUC) (X7) is the Education Index based on the adult literacy rate and the combined primary, secondary and tertiary gross enrolment ratio.
   Source: UNDP Human Development Report 2001
   <http://hdr.undp.org/reports/global/2001/en/indicator/indicator.cfm?File=indic_15_3_2.html>

8. ***Control Regimes*** (also CONTREG) (X8) corresponds to the country's membership to international treaties that control high technology exports, such as the Waasenar Agreement, which, for instance, put limits to exporting encryption software to certain countries.
   Source: SIPRI (Stockholm International Peace Research Institute) FIRST database 2002

9. ***Law Enf Intellig*** (also GOVSERV) (X9) is an estimate of secret/intelligence/military services and agencies per country in 2002 (an arbitrary point of one is given to all the countries, since it is presumed that every country has at least one such service).
   Source: FAS (Federation of American Scientists), Worldwide Intelligence and Security Agencies < http://www.fas.org/irp/world/index.html>

10. ***Secure Server1*** (also SECSERV) (X10) is the figure of secure servers (i.e. server computers that encrypt their files and are protected by firewalls, intrusion detection systems, IDS, and other methods). Secure servers are indispensable for electronic commerce, banking and financial services and for all those activities that require secure communications.
    Source: World Bank Indicators (WDI) database, 2001

11. ***Infrastr Index*** (also INFRASTR) (X11) is the infrastructure index which is the average of (a) ***Tel Lines Index*** and (b) ***Non Sec Servers Index***; (a) is the number of telephone lines per thousand inhabitants and (b) the number of non secure server computers (the figure is the total number of servers minus the secure servers). The formula for the index is ***Infrastr Index*** = (***Tel Lines Index*** + ***Non Sec Servers Index***)/2.
    Source: ITU (International Telecommunication Union), Free Statistics Homepage
    <http://www.itu.int/ITU-D/ict/statistics/>

The formula to calculate the CNO Index is = (X1+X2+X3+X4+X5+X6 X7+X8+X9+X10+X11)/11. Each single index is previously calculated as follow index = (actual value - observed min value)/(obs. max value - obs. min value). The method is akin to the one presented in UNDP (2001: 240/247).

APPENDIX B
Summary of Tables

****** Method 2 (covariance matrix) will be used for this analysis ******

R E L I A B I L I T Y A N A L Y S I S - S C A L E (A L P H A)

1.	CERT	Cert Teams Index
2.	TCHTRADE	Index of Technology Trade
3.	ESTUSER	Estimated User Index
4.	ENCRYPT	Encryption Software Index
5.	TECHSKL	Technical Skills Index
6.	ISP	Index of ISPs
7.	CONTREG	Control Regime Index
8.	GOVSERV	Intelligence Index
9.	EDUC	Education Index
10.	INFRAST	Infrastructures Index
11.	SECSERV	Secure Servers Index

		Mean	Std Dev	Cases
1.	CERT	.0337	.1331	59.0
2.	TCHTRADE	.2925	.2385	59.0
3.	ESTUSER	.3012	.3167	59.0
4.	ENCRYPT	.0503	.1392	59.0
5.	TECHSKL	.3438	.2342	59.0
6.	ISP	.0233	.1301	59.0
7.	CONTREG	.5220	.4594	59.0
8.	GOVSERV	.0926	.1648	59.0
9.	EDUC	.8793	.1189	59.0
10.	INFRAST	.2895	.2311	59.0
11.	SECSERV	.0250	.1302	59.0

Correlation Matrix

	CERT	TCHTRADE	ESTUSER	ENCRYPT	TECHSKL
CERT	1.0000				
TCHTRADE	.1690	1.0000			
ESTUSER	.3662	.3514	1.0000		
ENCRYPT	.9675	.1805	.4416	1.0000	
TECHSKL	.1537	.2369	.6363	.2232	1.0000
ISP	.9677	.1284	.3159	.9257	.1150
CONTREG	.2299	-.0074	.5485	.3070	.5419
GOVSERV	.7403	.0718	.2333	.7742	.2204
EDUC	.1939	.2361	.5909	.2336	.6563
INFRAST	.2135	.2492	.9199	.2837	.6062
SECSERV	.9806	.1475	.3321	.9429	.1336

R E L I A B I L I T Y A N A L Y S I S - S C A L E (A L P H A)

Correlation Matrix					
	ISP	CONTREG	GOVSERV	EDUC	INFRAST
ISP	1.0000				
CONTREG	.1736	1.0000			
GOVSERV	.7509	.2580	1.0000		
EDUC	.1358	.6121	.0667	1.0000	
INFRAST	.1503	.6301	.1062	.6721	1.0000
SECSERV	.9955	.1922	.7630	.1535	.1697

N of Cases = 59.0

Statistics for Scale	Mean	Variance	Std Dev	N of Variables
	2.8533	2.4186	1.5552	11

Item-total Statistics				
	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Alpha if Item Deleted
CERT	2.8196	2.1666	.5983	.8182
TCHTRADE	2.5608	2.1974	.2324	.8422
ESTUSER	2.5521	1.6844	.7710	.7889
ENCRYPT	2.8030	2.1294	.6641	.8140
TECHSKL	2.5095	1.9678	.6026	.8096
ISP	2.8300	2.1937	.5396	.8215
CONTREG	2.3313	1.5821	.5412	.8458
GOVSERV	2.7607	2.1617	.4740	.8224
EDUC	1.9740	2.1808	.6370	.8183
INFRAST	2.5638	1.9080	.7161	.7993
SECSERV	2.8283	2.1844	.5646	.8202

R E L I A B I L I T Y A N A L Y S I S - S C A L E (A L P H A)

Reliability Coefficients 11 items

Alpha = .8322 Standardized item alpha = .8831

APPENDIX C
Infowar Index and ranking of Countries[#]

COUNTRIES	INFOWAR INDEX	RANK
BANGLA DESH	n.a.	n.c.
BELGIUM	n.a.	n.c.
BRUNEI	n.a.	n.c.
BULGARIA	n.a.	n.c.
CHILE	n.a.	n.c.
HONG KONG	n.a.	n.c.
IRAN	n.a.	n.c.
IVORY COAST	n.a.	n.c.
LEBANON	n.a.	n.c.
LUXEMBOURG	n.a.	n.c.
MADAGASCAR	n.a.	n.c.
NEPAL	n.a.	n.c.
QATAR	n.a.	n.c.
SAUDI ARABIA	n.a.	n.c.
SWAZILAND	n.a.	n.c.
TAIWAN	n.a.	n.c.
UKRAINE	n.a.	n.c.
UAE	n.a.	n.c.
VENEZUELA	n.a.	n.c.
YUGOSLAVIA	n.a.	n.c.
UNITED STATES	0.86	1
AUSTRALIA	0.48	2
FINLAND	0.46	3
UNITED KINGDOM	0.45	4
SWEDEN	0.44	5
CANADA	0.43	6
NORWAY	0.41	7
NETHERLANDS	0.40	8
DENMARK	0.40	8
GERMANY	0.39	9
KOREA ROK	0.38	10
SWITZERLAND	0.37	11
IRELAND	0.37	11
SINGAPORE	0.37	11
JAPAN	0.36	14
FRANCE	0.36	14
NEW ZEALAND	0.35	16
AUSTRIA	0.34	17

[#] "N.a." and "n.c." in the table stand for not available and not computed. Since some of the values for the 11 indicators were missing for some countries, SPSS could compute the ranking for those countries and excluded them from the table.

ICELAND	0.33	18
SPAIN	0.32	19
ITALY	0.31	20
GREECE	0.30	21
RUSSIA	0.29	22
HUNGARY	0.28	23
PORTUGAL	0.27	24
CZECH REP.	0.27	24
ARGENTINA	0.26	26
POLAND	0.24	27
ISRAEL	0.24	28
SLOVENIA	0.24	28
SLOVAKIA	0.24	28
ESTONIA	0.23	31
ROMANIA	0.22	32
MALTA	0.21	33
TURKEY	0.21	33
MALAYSIA	0.19	35
CYPRUS	0.19	35
PHILIPPINES	0.18	37
LATVIA	0.18	37
SOUTH AFRICA	0.18	37
MEXICO	0.18	37
BELARUS	0.17	41
BRAZIL	0.17	41
LITHUANIA	0.16	43
CHINA	0.16	43
CROATIA	0.15	45
THAILAND	0.15	45
INDONESIA	0.12	47
COLUMBIA	0.11	48
PERU	0.11	48
ARMENIA	0.11	48
NIGERIA	0.11	48
KUWAIT	0.11	48
INDIA	0.10	53
OMAN	0.09	54
ZIMBABWE	0.08	55
KENYA	0.07	56
GHANA	0.07	56
PAKISTAN	0.06	57