

Securing the Information Age

The Challenges of Complexity for Critical Infrastructure Protection and IR Theory

Forthcoming in: Johan Eriksson and Giampiero Giacomello (eds.) “International Relations and Security in the Digital Age”, London: Routledge.

Myriam A. Dunn

Center for Security Studies, ETH Zürich, 8092 Zurich, Switzerland

INTRODUCTION

By aiming to evaluate the strengths and limits of IR theory in order to gain an understanding of security in the digital or information age, we take on an exceedingly difficult task. Not only has this issue hardly ever been addressed before, leaving us with barely any literature to base our analysis on – we also enter a realm of vast extent, indistinct boundaries, and a sloppy conceptual arsenal. There are more questions of the basic sort than answers: What *is* information age security and how might it be defined in a meaningful way? Is there really anything *new* about information age security that clearly sets it apart from more traditional security matters? Which specific aspects of information age security do we want to explain and why? And, maybe the most challenging question in the context of this project: is a theory of the information age needed at all?

Due to the vocabulary of clichés that inhabits the information age debate, we must place particular emphasis on conceptual precision in order to arrive at meaningful analysis. Absent any satisfactory definition of “information age security”, we must fill the concept with meaning by designating issues that could be part of it. It is sensible to discern two categories: *offensive*

activities such as information warfare, cyber-crime, or cyber-terrorism (Libicki 1999; Cohen 1996: 39; David 1997; Cooper 1997; Parker 1983; Lewis 2002; Pollitt 1997); and *defensive* activities such as defensive information operations, information assurance, or critical information infrastructure protection (CIIP) (Libicki 1995; Dunn and Wigert 2004; Dunn and Mauer 2006). The common denominator of these issues is their unspecified connection to the so-called information revolution and cyberspace, or, more specifically, their connection to the so-called information infrastructure.

However, it is not easy to understand what exactly the information infrastructure is. This is due to the fact that it has not only a *physical* component that is fairly easily grasped – such as high-speed, interactive, narrow-band, and broadband networks; satellite, terrestrial, and wireless communications systems; and the computers, televisions, telephones, radios, and other products that people employ to access the infrastructure – but also an equally important *immaterial*, sometimes very elusive (cyber)-component, namely the information and content that flows through the infrastructure, the knowledge that is created from this, and the services that are provided (Dunn and Wigert 2004: 19-20). Furthermore, it would be misguided to restrict “information age security” to cyber-attacks or incidents or, conversely, to cyber-targets, because the means of attack can be both physical (such as a backhoe to sever a telecommunications cable, or explosives) and virtual (such as electromagnetic pulse or hacker tools) (OCI-PEP 2003: 12; Devost et al. 1997: 76).

It is striking that all the issues named above are very ambiguous concepts, each one with its own string of varying definitions. As a basis for theorizing, this situation is not satisfactory. In fact, it is doubtful whether the label “information-age security”, or any similar term, is practical at all due to its imprecision. In order to lay the foundations for theorizing, therefore, we must first carefully identify what precise aspects of the phenomenon we want to explain for what reasons. It is clear, furthermore, that the scope and nature of a possible theory for as-

pects of the information age depends on how we perceive and interpret the magnitude and depth of the current transformations. Such theorizing might either aim to be thoroughly “new” if the current transformation is thorough and sweeping – or it might be considered satisfactory to adapt old approaches to specific circumstances if changes are less thorough.

By setting out to answer what IR theory has to offer in terms of explanations for security in the information age, “information-age security” is in fact automatically and uncritically regarded as a specific phenomenon that establishes a specific context with a specific impact and thus creates the need for new approaches. However, it is doubtful whether this is actually the case. Below, we first set out to understand what makes the information age special and what its defining features are. From there, we go on to describe what this means for international relations. We will show that states mainly focus their attention on the protection of critical (information) infrastructures due to a very particular information-age threat image. Notwithstanding this trend, we argue that the forces of the information revolution have not changed the conditions of security, defined in an objective sense as the absence of threat to a society’s core values and in a subjective sense as the absence of fear that these values will be attacked (Wolfers 1962; Baldwin 1997: 13). What has changed significantly due to the particularities of the information age, however, are some of the conditions for *securing*.

The distinction between security and securing is slight but pivotal; while *security* is a momentarily static condition, *securing* has a somewhat differing connotation: it includes the act of making something safe or secure and thus of actively thwarting possible threats to any given referent object of security, implying actors, politics, and policies. Due to the information revolution, we can observe a qualitatively significant change in the (perceived) nature of threats or risks to security, a change in some of the means to achieve the goal of security, and a change in the constellation of actors involved in the securing process. We then show that the defining key feature of the information age, underlying all of these observations, is the pre-

dominance of complexity and change on two levels: 1) on the level of technological systems and 2) on the level of the international system.

From the field of complexity studies, a research area belonging to the natural sciences, we learn about the behaviour of systems in general, and speculate on the consequences of this in the third sub-chapter. However, while complexity theory offers answers to certain questions concerning the technical systems, we argue that the applicability of these ideas is somewhat limited for the political realm. The main reason for this is that from a constructivist vantage point, the information revolution and ensuing complexity only matter when they are perceived to matter. They are nothing more than conditions that shape the threat perception of key decision-makers and thus have an impact on their thoughts and actions.

INFORMATION-AGE LITERATURE SCRUTINIZED

There is little doubt among experts that the basic conditions of international relations have changed in the last decade, with the *information revolution* often named as one major driver of change (Zacher 1992: 58-59; Castells 1996). But what *is* this famed information revolution, and what makes it so special? It is common knowledge that the significance of information is not unique just to our time, but that it has always been vital to humankind. It is also commonly understood that throughout history, advances in scientific-technical fields have played major roles in changing human affairs, and that there have been other information and communication revolutions, all of which significantly shaped history, human activities, and their institutions (Papp et al. 1997; Waldrop 1998; Deibert 1997; Hobart and Schiffman 2000; Borgmann 1999; Freeman and Louca 2002).

When probing phenomena that have been drained of meaning by overuse, researchers must be particularly careful not to fall into the trap of re-inventing the wheel or calling everything “new” just because it appears so at first sight. They should rather strive to see things in their

proper historical context and advance to the core of things by meticulously analysing what exactly sets this development apart from other developments. Such an undertaking is hampered by imprecision in terminology: “Information revolution” or “information age” are terms currently used by many different parties for many different facets of an elusive phenomenon, leaving the researcher with a confusing diversity of usually poorly defined concepts (Fisher 2001; French 2000). The nature of these terms is such that they have never been precise in their meaning – nowadays, however, they have been used so extensively that they can basically mean everything, and are thus ultimately devoid of meaning altogether. But even though the terms have become mere catchphrases, there is simply no alternative to their use.

In our view, the current “revolution” concerns a special set of technologies, often subsumed under the heading of information and communication technologies (ICT) (Alberts et al. 1997). In particular, the marriage of computers and telecommunications and the ongoing and dynamical integration of these technologies into a multimedia system of communication with global reach are defining features of the current technological development. This adds a great deal of speed, capacity, and flexibility to the gathering, procession, and transmission of data into knowledge, and enhances humankind’s ability to communicate, to utilize information, and to overcome obstacles earlier presented to communication by distance, time, and location (Dunn 2002: 59-64).

To advance from here on and begin to interpret what this technological expansion actually means for the individual, society, the state, or international relations implies a great deal of speculation. Even if certain ramifications seem evident, there is almost no empirically grounded research that would allow us to convincingly move beyond the anecdotal evidence that is frequently offered. Nonetheless, in order to determine what the international community believes to be the key characteristics of the current revolution, we recapitulate the main arguments from the information revolution literature below.

The Changing Nature of Power

At the core of these writings lies the notion that we face changes in the nature and quality of power. Power in politics is often divided into three subsections: economic, military, and political power. These are the three pillars on which the ability of nation-states to achieve their goals rests. Economic power is derived from the resources within a state's borders and the aptitude to trade them, military power comes from the availability of people and material, and political power is drawn from the potency of leaders and institutions, the people's support, and endorsements from other nation-states (Rothkopf 1999: 325-26). The traditional view of Realist political science, in a basic form, is that military power dominates other forms of authority, and that the states with the most military power therefore dominate world affairs. This interpretation of the Realist school was critically confronted as early as 1977, mainly as a reaction to observations about a changing economic world (Keohane and Nye 1977). Since then, the resources that produce power capabilities have become even more complex; today, the three "pillars of power" are being shaken by the growing influence of information and communication technology (ICT) on international relations.

Control over knowledge, beliefs, and ideas is increasingly regarded as a complement to control over tangible resources such as military forces, raw materials, and economic productive capability. Often, one hears that "information is power" (Nye and Owens 1996). In a political-science view, this is the case because information reduces uncertainty and can result in an asymmetrical advantage over others that have less information at their disposal. ICTs, which help to accumulate information that can be turned into knowledge, are therefore today's ultimate and most important power resource. Economic instruments, too, have gained importance for the exercise of power. This mainly empowers multinational corporations and other business entities. The most influential and most frequently cited article on the topic is Keohane

and Nye's "Power and Interdependence in the Information Age" (Keohane and Nye 1998; Nye 1990).

The Relative Power Loss of State Actors

It is frequently argued that the main locus of power resources has shifted from military, to economic, and now to informational resources, as noted in the previous chapter. Transfer of authority occurs in diverse directions through "framegrative" dynamics (Rosenau 1998), creation of wealth today happens through ideas, knowledge, and opportunity. Power increasingly flows to centres of innovations and technological know-how, and – on the individual level – to a new kind of technological elite, those specialists who control or master ICT through extraordinary skills or ideas. There are two central conflicts that reveal the nature of the ongoing redistribution of power: first, the idea that the emergence of a global electronic marketplace will bring about the inevitable collapse of the state's economic pillar of power, as companies increasingly become global citizens and economic boundaries no longer correspond to political ones (Rosecrance 1999); and second, the notion that the information revolution empowers new forms of international actors, thus challenging the state's status as the major player in the international system (Papp and Albert 1997).

The information revolution is not only seen to affect the role and position of states, but also the position and influence of other actors in international affairs. These are mainly international governmental organizations (IGOs), multinational corporations (MNCs), and non-governmental organization (NGOs). It further exerts considerable influence on the role of the individual: The strengthened position of the individual can be explained by the expansion of the individual's diagnostic capabilities thanks to the advance of ICT, which allow citizens to become more competent and enhance their analytical skills. This development has been labelled "skill revolution" (Rosenau 1998: 42-45).

The outcome of this rearrangement will likely be a skewed, complex, and volatile pattern of power distribution, as transfer of authority occurs in diverse directions and changes are absorbed and operationalised by different actors at different levels in different ways and at different speeds. The final result of such a development, it is assumed, will be a “bifurcation” of global structures into state-centric and multi-centric subsystems where states are no longer the only key actors (Rosenau 1990; Nye 1998). In order to express the complex and ambiguous nature of the development, neologisms like “fragemegration” (fragmentation/ integration) or “glocalization” (globalization/ localization) have been created (Rosenau 1998).

FROM QUANTITATIVE CHANGE TO QUALITATIVE CONSEQUENCES

Even though many of the claims concerning changing power structures ring true in some way, most of them are based on the premise that more information and communication technologies automatically imply a qualitative difference. However, even if we count the numbers of computers connected to the Internet, the use of mobile phones in percentage of the overall population of a country, or the size of information available on the World Wide Web, no convincing conclusion is possible as to their impact. Quantities are undoubtedly important, but it is only our attribution of *meaning* to them that will allow us to truly theorize about the information age. As Kai Holsti writes, meaning is the link connecting quantitative changes (causes) to qualitative changes (consequences) (Holsti 1998: 5). Unless we attribute meaning to quantities, we have no way of knowing when change becomes significant, or when it is or becomes truly transformational. In fact, one could argue that a new theory is only required if we establish that there is such a fundamental change in the environment that old approaches no longer hold true.

When we turn to IR theory, we find that even though the arguments about the nature of change, its possibilities, and its consequences are implicit in the great debates among theorists of IR and thus constitute a major area of disagreement, the issue has been largely neglected in

the mainstream literature in this field (Buzan and Jones 1981; Ruggie 1993; Holsti 1998). However, (new) institutionalist approaches offer an interesting approach to the topic of change: If we view the international system as an ensemble of institutions, which can be defined as practices constituted by norms or rules (Kratohwil 1989: 64), one might argue that a fundamental change in the international system occurs when a significant part of its constitutive norms or rules are altered. Susan Strange has argued similarly, stating that technological changes only change power structures if they are accompanied by changes in the basic belief systems which underpin or support the political arrangements acceptable to society (Strange 1988: 123). The key question in connection with our topic can therefore be rephrased as follows: Have quantitative changes induced by the information revolution produced a significant amount of new patterns, norms, practices, or institutions so as to cause a fundamental qualitative change in the international system?

There is no simple answer to this question, for a number of reasons that are conceptual as well as empirical: *First*, these developments are recent and ongoing, and difficulties in grasping their true proportions are inevitable, because we are in the midst of the process ourselves. *Second*, the implications are far from straightforward: Many observers have pointed out that complexity and change are the two defining characteristics of the information age, since the present epoch is marked by persistent opposites and derives its order from episodic patterns with very contradictory outcomes (Rosenau 1990; CSIS 1996). It is therefore very difficult to produce stringent empirical evidence for or against the claim that international institutions have changed. *Third*, the above question refers to a systemic and sweeping phenomenon, a fundamental type of change that transforms the practices and constitutive conventions of the entire system. This universalism is the hallmark of almost every conventional international relations theory. However, in the light of the fact that developments are not only ongoing, but also very ambiguous, a context-dependent approach is more appropriate. *Fourth*, and most

importantly, we believe that the *perception* of these changes is what truly matters, and not their objectively measurable reality. Hence, in the following, we focus on qualitative consequences with empirically observable effects on securing practices.

Broadening of the Threat Spectrum

First and foremost, the information revolution is directly responsible for the rapidly increasing number of forewarnings in the 1990s concerned with information age security (Eriksson 2001b). There are two sides to the particular information-age threat image: A new kind of vulnerability due to dependency of modern society's on inherently insecure information systems on the one hand, and the aforementioned redistribution of power on the other:

- Due to falling costs, increased and large-scale availability, greater utility, and ease of use, ICT has vastly propagated into all aspects of life, with the result that societies in developed countries are becoming increasingly dependent on them for their well-being, everyday life, work, economic transactions, comfort, entertainment, and many personal interactions (Dunn 2002: 62-65).
- The perception today is that there are a variety of actors in the cyber-environment who are willing to contravene national legal frameworks and hide in the relative anonymity of cyberspace. The growing prevalence and aptitude of these cyber-based threat actors is seen as considerable threat to national security, because they seem to have the capacity to inflict significant damage through tools that are readily available and relatively easy to use by those with even a cursory knowledge of, and skill in using, computer technologies (PCCIP 1997).

These two aspects together feed the fear of severe *asymmetrical vulnerabilities*, a concept extensively discussed in the United States (Blank 2003; Metz and Johnson 2001: 2; Husain 2003; Berkowitz 2003). The word "asymmetry" is used to describe a broad range of threats

and tactics; at the core of the term is the intention to circumvent the opponents' advantage in capabilities by avoiding their strengths and exploiting their weaknesses (Kolet 2001). The concept of asymmetric threat or vulnerability connotes that "the enemy", clearly doomed to fail against the mighty US high-tech war machine in any conventional conflict, will instead plan to bring the US to its knees by striking at vital points at home (Berkowitz 1997) – these points being fundamental to the national security and to the essential functioning of industrialized societies as a whole, and not necessarily to the military in particular. These vital points are called "critical infrastructures" (CI) in today's security debate.

The concept of critical infrastructures usually includes sectors such as information and telecommunications, financial services, energy and utilities, transport and distribution, plus a list of additional elements varying across countries and over time (Moteff 2002; Dunn and Wigert 2004; Abele-Wigert and Dunn 2006). Attacking infrastructure has a "force multiplier" effect, allowing even a relatively small attack to achieve a much greater impact. Because the CI delivers a range of services that individuals, and society as a whole, depend on, any damage to or interruption of the CI causes ripples across the technical and the societal systems. For this reason, CI structures and networks have historically proven to be appealing targets for a whole array of actors (OCIPEP 2003).

In fact, protection concepts for strategically important infrastructures and objects have been part of national defence planning for decades, though at varying levels of importance. Towards the end of the Cold War and for a couple of years thereafter, the possibility of infrastructure discontinuity caused by attacks or other disruptions played a relatively minor role in the security debate – only to gain new impetus around the mid-1990s, due to the information revolution (Luijff et al. 2003). Since then, critical infrastructure protection (CIP) as a policy issue has risen to the top of the security agendas of many countries in the last couple of years.

The information infrastructure plays a very special role in the CIP debate. Vulnerabilities in critical infrastructures are believed to be on the rise mainly because the information infrastructure underpins many elements of the critical infrastructure, which therefore become dependent on a spectrum of highly interdependent national and international software-based control systems for their smooth, reliable, and continuous operation (Moteff et al. 2003; Rathmell 2001). This, in turn, leads to increasingly complex interdependencies. This part of the global or national information infrastructure, which is essential for the continuity of critical infrastructure services, is called *critical information infrastructure* (CII) in the debate.

The increasing value of information and the availability of electronic means to manage its ever-growing volume have not only made information and information systems an invaluable asset, but a lucrative target, too. Information systems are exposed to failures, are attractive targets for malicious attacks, and are susceptible to cascading failures. The interdependency factor means that critical infrastructures do not need to be attacked physically, but may be targeted through electronic or virtual means, the worst-case scenario being a concerted action by qualified hackers with hostile intentions that could force a whole nation to its knees (PCCIP 1997: 5-8). This is seen as a particularly worrying prospect because the “enemy” becomes a faceless and remote entity, a great unknown that is almost impossible to track and that opposes security institutions and legal systems that are ill-suited to counter or retaliate against such a threat.

As a qualitative consequence of the second order within the information revolution, this particular threat image causes very specific reactions in the form of critical infrastructure protection policies. This circumstance, in turn, has led to the situation where CIP or the securing of the information age lies at the heart of the “information-age security” debate.

Complexity as a Key Feature of Systems

A second qualitative consequence of the information revolution is complexity. It is an uncontested assumption that complex problems are on the rise in, and due to, the information age. One possible explanation for complexity in the technical world can be found in the combination of two laws of technical innovation, namely Moore's Law and Metcalfe's Law, which are widely credited as having provided the stimulus that has driven the stunning growth of Internet connectivity (Moore 1965; Metcalfe 1995; Downes et al. 1998):

- Moore's Law states that the number of transistors per square inch on integrated circuits will double approximately every 18 months, which means that computing power rises exponentially over time.
- Metcalfe's Law states that the value of a communication system grows as the square of the number of users of the system, which implies an increasing number of networks, nodes, and links.

According to one simple but straightforward definition, complexity is the sum of interdependencies plus change (Cf. Gomez 2001: 151). This means that complexity in information infrastructure systems is increasing, as an exponential technological development leads to change and brings forth an increasing number of networks, nodes, and links to growing interdependencies. In addition, the complexity of these systems grows with the extension of the geographical reach and the expansion of the services provided, the introduction of new components with richer functionality using diverse technologies, and the layering of systems over systems (Kyriakopoulos and Wilikens 2000; Masera and Wilikens 2001).

Mainly as a consequence of their interactions with the information infrastructure, the critical infrastructures are being composed into networks-of-networks of different sizes. Three main, interrelated trends affect these infrastructures: 1) their increasing complexity, with an accel-

eration that reflects the general evolution of technology; 2) their interconnectedness, put into practice at different layers: organizational, procedural, informational, material; and 3) a growing reliance on ICT, both for internal use and for interaction with external systems (Masera and Wilikens 2001). Therefore, infrastructures are complex and interdependent systems, and it is not possible to control their full range of interaction with the surrounding, pre-existing technical and social environments.

System complexity has two immediate consequences for the topic of critical infrastructure protection. First, a well-known theory claims that technological systems that are interactively complex and tightly coupled will be struck by accidents that cannot be prevented. Because of the inherent complexity, independent failures will interact in ways that can neither be foreseen by designers nor comprehended by operators. If the system is also tightly coupled, the failures will rapidly escalate beyond control before anyone understands what is happening and is able to intervene (Perrow 1984; Turner and Pidgeon 1997). This overall pessimistic perspective on accidents and the limited possibilities of preventing them and coping with them resonates in much of the information age security debate.

Second, the dynamic interactions of complex, decentralized, open, unbounded (technical) systems amounts to an overtaxing of abilities to articulate and evaluate the problem, thus creating a practical challenge for those involved in drafting measures for securing. As Forrester showed back in the early 1960s, complex systems behave contra-intuitively due to parallel occurrences happening at different speeds, irregularities, and non-linear cause/effect relationships, with the result that the human brain is unable to “read” these systems correctly (Forrester 1961). Besides, the tools currently available for evaluation of these systems are inadequate; the “methodological toolbox” in use is filled with old tools that have, in some cases, been hurriedly adapted to a new set of problems (Dunn 2004; Dunn 2005; Dunn 2006). However, both the systems and the risk environment have become qualitatively different in a way

that demands new analytical techniques and methodologies for their evaluation (Allen and Sledge 2002).

Furthermore, it has become almost conventional wisdom today that “the world”, or to put it in IR terms, the international system, has also become more complex. The main reason usually given for this is the growing number of independent international and transnational actors playing power games on multiple levels evolving around national, regional, and global dynamics (Jervis 1997a, 1997b). Complexity is thus seen as a consequence of there being more actors in the international system. In addition, the observation that the present epoch is marked by persistent opposites and derives its order from episodic patterns with very contradictory outcomes is seen as a sign of increasing complexity (Rosenau 1990).

The feeling of increasing complexity on a higher system level is closely linked to the fact that the intellectual tools presently available to probe the pervasive uncertainty underlying our emergent epoch are not sufficient to the task. In that sense, complexity and the overtaxing of our abilities is more than a mere practical problem for those involved in the securing of the information infrastructure. In fact, we can argue that the world has *always* been complex, but it has been one of the aims of IR theory to render it more intelligible by simplifying it. The most nefarious consequence of Waltz’s legacy of an uncompromising search for a universal, parsimonious theory has in fact been that mainstream IR theory *cannot* account for complexity and the closely connected concept of change.

THEORETICAL AND PRACTICAL IMPLICATIONS

At least since the development of Shannon and Weaver’s information theory (Shannon and Weaver 1949), formal, semi-formal, or informal notions of “complexity” have been used to express properties of objects and processes in a variety of fields. Despite or maybe because of the diversity of scientific efforts involved in this work, little agreement has been reached on

what, precisely, complexity entails, or how a general notion of complexity may be systematically applied to various fields of research (Butts 2001; Çambel 1992: xi). In addition, many different kinds of complexity, such as logical, relational, semiotic, computational complexity, are distinguished (Biggiero 2001; Casti 1979), so that the problem does not end when appropriate definitions are found, but extends to the issues of measurement and the understanding of implications.

One prominent field of research that suggests itself for determining how complex systems behave, is that of *complexity studies*, a branch of chaos theory. “Chaos theory” is a grab-bag expression for a whole set of studies, an amalgam of different techniques of mathematics and science concerned with order and pattern where formerly only the random, erratic, and unpredictable had been observed (Gleick 1987; Kellert 1995). The difference between chaos and complexity theory is not entirely clear-cut, but we can state that chaos theory mainly deals with situations such as turbulence that rapidly become highly disordered and usually unmanageable, whereas complexity studies deal with systems whose behaviour may be hard to predict, but have a good deal of structure (Axelrod and Cohen 1999: xv). The notion of systems is the founding stone of the “new sciences”, and the larger framework that brought forth chaos theory is the so-called theory of *dynamical systems* (Crutchfield et al. 1986). Complexity studies are in fact applicable to all kinds of systems, regardless of their size or nature, so that the following is universally applicable both to technological (sub-) systems and to the international system.

Complexity Studies and the Behaviour of Complex Systems

According to the usual definitions, complex systems are complex insofar as they incorporate a number of variables that simultaneously play many different roles in the system’s evolution and following many different laws of behaviour (Cohen 1995: 88). Complexity is expected to arise as a natural development when a system reaches a certain level of variety and diversity

because of many simple components interacting simultaneously. The complexity is thus actually in the organization, more precisely, in the myriad possible ways that the components of the system can interact. Therefore, its behaviour is not predictable from knowledge of individual elements but can only be discovered by studying how these elements interact and how the system adapts and changes throughout time (Waldrop 1992: 86). Complex phenomena can also occur in relatively simple systems with very few variables. Or, put differently, simple rules and simple initial conditions can give rise to the most complex behaviour (Merry 1995).

One of the fundamental issues of complexity is the nature of order and organization (Bosomaier and Green 2000: 6). In complexity theory, the appearance of new order is explained through the concept of *self-organization*, which connotes a spontaneous formation of a stable, but complex pattern out of seemingly random entities (Foerster and Zopf 1962; Ashby 1962; Bak 1996). In general, self-organization refers to an evolutionary process in which the internal organization of a system increases automatically without being guided or managed by an outside source. Self-organization is triggered by internal variation processes, which are called “fluctuations”: Over time, complex systems become increasingly sensitive to internal and external fluctuations – and the more complex a system is, the more sensitive and vulnerable to fluctuations it becomes (Merry 1995: 65; Prigogine 1981). At a certain point, these fluctuations pass a critical threshold, also called a *bifurcation point*, and then, following a transitional stage of chaotic fluctuations, completely reorganize the entire system (Laszlo 1991).

The ability of a system to evolve in such a way as to approach a critical point and then maintain itself at that point is called *self-organized criticality*. Bak, who coined the term, argues that complex behavior in nature reflects the tendency of large systems with many components to evolve into a poised, “critical” state, highly imbalanced, where minor disturbances may lead to events, called avalanches, of all sizes (Bak 1996). This means that complex systems tend to adapt to, or are themselves on, the edge of chaos and most of the changes take place

through catastrophic events rather than by following a smooth gradual path – the new path the system will take cannot be predicted and controlled (Ibid.).

Complex systems further show surprising and unexpected behaviour that is a property of the system as a whole. Often, they self-organize in an evolutionary process in which the internal organization of a system increases automatically without being guided or managed by an outside source (Crutchfield 1994). Structures can emerge both through the influence of emergent phenomena on the various parts of a system, such as the effect of norms on individuals, and through the emergence of entirely new dynamics within the system (Mihata 1997: 33). Due to the emergent behaviour, the complex system cannot be understood by reducing it to its parts; moreover, the behaviour we are interested in evaporates when we try to reduce the system to a simpler, better-understood one (Bar-Yam 1997: 11).

That complexity theory is highly relevant to the CIP debate is clearly discernible from the fact that multi-million dollar efforts are currently under way at the US National Infrastructure Simulation and Analysis Center (NISAC) to develop computer simulation tools that can predict, in real time, the consequences of disruptive events on a nation's critical infrastructures. The modelling approach utilizes an agent-based methodology to predict critical infrastructure interactions. It treats infrastructures like *Complex Adaptive Systems* (CAS), which are populations of interacting agents where an agent is an entity with a location, capabilities, and memory (Rinaldi et al. 2001). With this perspective, each component of an infrastructure constitutes a small part of the intricate web that forms the overall infrastructure. This viewpoint incorporates benefits for modelling and simulation, and it is hoped that such approaches will be able to explain (some) emergent behaviour of large-scale critical infrastructures.

Limits of the Complexity Paradigm

Apart from being directly applied for the modelling of complex interdependencies, chaos theory and its various strands, developed in a natural sciences context, are also increasingly being applied to the social sciences. What the new science seem to have done is to place within our grasp a set of very powerful intellectual tools and concepts to think with, which appear to be free of many of the limitations of the traditional approaches. New concepts, such as emergence, become conceivable, and new methods, such as nonlinear computer modelling, suggest themselves as legitimate modes of study (Eve et al. 1997: xxi; Byrne 1998; Cederman 1997; Cederman and Gleditsch 2004; Alberts and Czerwinski 1997). Given the fundamental differences between physical and social systems, various authors have explored the validity of applying the conceptual and methodological tools of chaos theory to social systems (cf. Albert 1995a; Eve et al. 1997; Turner 1997). Most of these writings come to the conclusion that this exchange can be very fruitful, if one is aware of the dangers of abusing concepts from other disciplines, such as chaos theory, or extending them by false and farfetched analogy to support existing theories or normative views (Albert 1995b: 2; Michaels 1995).

However, the hopes that complexity theory may somehow point the way to a course of action which can ameliorate the uncertainties inherent in a complex world have been disappointed, mainly because the benefits have been exaggerated (Bak 1996: 43-44; Rosenau 1997). Another major problem is that the application of the mathematics of chaos, of genetic algorithms that manipulate precise numerical data through explicit operational rules, and of nonlinear dynamics requires quantification and availability of lengthy time-series data (Kellert 1995). Since human actions and cultures can never be so clearly encapsulated, the question is whether the chaos paradigm is even methodologically accessible at all to scholars in the humanities (Cohen 1995).

In addition, there are severe limitations to the system paradigm that the whole construct of the new sciences depends on. One problem is the inherent automaticity in systemic thinking. To see a system as if it were a living organism in which things happen without outside influence fails to take into account the most central parameter of the social world: the actor, or more explicitly, the freedom of the actor to act. The main problem, however, is one of system ontology: calculation and modelling inherently rely on our ability to define the variables of the system. This is dependent on our ability to describe the system, or more specifically, on our ability to describe the system *boundaries*: However, the designation of factors as being external (exogenous) or internal (endogenous) with regard to a system depends largely on the viewpoint of the observer (Bertalanffy 1968: 141).

Ultimately, all boundaries are dynamic rather than spatial. Hence, an object – and in particular, a system – is definable only by its cohesion in a broad sense, that is, by the interactions of the component elements (Bertalanffy 1975: 165-166). But how can we know whether a variable is present in a system, unless we already know all the variables it interrelates with? Interactions or interrelations are never directly seen or perceived; they are always conceptual constructs. This means that no meaningful distinctions can be drawn between “real”, observable objects and systems on the one hand, and “conceptual” constructs and systems on the other.

Lessons and Implications of the Complexity Paradigm

But even though we might not be able to define system boundaries, we can draw some lessons for the topic of information age security from the complexity paradigm. Complex systems exhibit a number of specific, non-exclusive features and behaviours, from which some lessons can be drawn, without falling into the trap of domesticating “real-world demons in ill-fitting complex cages” (Bowker 1993) or of abusing metaphors. As described above, both the inner workings and the external manifestations of systems are characterized by interrelation. This means that complex systems cannot exist in isolation – by their very nature, they are tied to

and connected to other systems, and couple together to create higher order systems. This means that results cannot be predicted from the separate actions: the effect of one variable depends on the state of another. We can also argue that strategies depend on the strategies of others. Interactions between strategies occur when actors consciously react to others and try to anticipate what others will do. Both the success and failures of policies are therefore determined interactively (Jervis 1997a; Axelrod 1997).

Furthermore, non-linear behaviour is one of the cornerstones of complexity, as it creates unpredictability, uncertainty, and volatility in the system. Cause and effect, or inputs and outputs, are not proportional; the whole does not correspond to the sum of its parts, or are even qualitatively recognizable in its constituent components. This means that behaviour changes the environment: initial behaviour patterns and outcomes often influence later ones, producing powerful dynamics that explain change over times and that cannot be captured by labelling one set of elements “causes” and other “effects” (Jervis 1997b). In other words, initial conditions have an impact on the outcome of the events. Tiny causes can have enormous effects. Small uncertainties are amplified, so that even though the behaviour is predictable in the short term, it is unpredictable in the long term (Merry 1995: 26-27). Extreme sensitivity to initial boundary conditions or historical paths makes detailed prediction impossible (Mihata 1997: 33-34). Because specific dynamic system outputs cannot be predicted (in the long run), it is not possible to plan, via prediction, the outcomes of an intervention in a social system (Michaels 1995: 23).

The first implication of the complexity paradigm is therefore mainly methodological by nature, since the underlying assumption, which views the current environment as being interactive to a degree as to inhibit the tracing of causal sequences, obviates the framing of hypotheses that link independent and dependent variables. The presumption that certain phenomena (the independent variables) are prior in time to those they affect (the dependent variables)

may be valid in a short-term context, but it may not hold in a stretched-out time perspective (Rosenau 1992: 17-18). We should therefore switch our attention from outcomes to *processes* (Michaels 1995), which is also the remedy proposed by some constructivists to overcome the agent-structure problem (Kratochwil 1989).

However, complexity, whether on the technical system level or on a higher, international level, is, again, inherently a matter of perceptions. Views that abolish the concept of objective reality also dissolve the idea of intrinsic complexity, meaning that complexity is not an intrinsic property of an object, but rather depends on the observer (Casti 1996: 7). This means that no matter whether or not an objective reality exists, it is approachable only through social definitions. Individuals do not respond to the (probably existing, objective) reality directly, but through socially constructed thought frameworks. In theoretical terms, this means that complexity, if perceived by decision-makers or other influential actors to be a problem, will influence the threat perception of key actors and their subsequent actions (Eriksson 2001a).

The same is true for the observation made above that there are more actors on the international stage today, wielding more influence due to the skills revolution, and with more knowledge at their disposal. Based on the premise that decentralized network-based soft power structures have gained in importance, the argument runs that the state's monopoly on authority has become fragmented, and a plethora of non-governmental organizations, social movements, and other transnational non-state networks are now competing with states for influence (Papp et al. 1997; Nichiporuk and Builder 1997).

In CIP, we can observe that governments can no longer “go it alone”: In securing the information age, governments are challenged to operate in unfamiliar ways, sharing influence with experts in the IT community, with businesses, and with non-profit organizations, because the ownership, operation, and supply of the critical systems are in the hands of a largely private

industry, which is diverse, intermixed, and relatively unregulated (Baird 2002). Collectively, this industry has far more technical resources and operational access to the infrastructures than the government does, so that ultimately, the private sector will have to do most of the work and must bear most of the burden to make infrastructures more secure (Goodman et al. 2002; Bosch 2002). As a result, the process of policy-making is becoming more and more open and is being transformed from a single-entity phenomenon to a multi-entity one, as it has become customary to involve representatives of all major stakeholders in the policy preparation process (O'Brien et al. 2003).

Clearly, what matters is not whether the change in power is objectively “true” or not, but whether states are willing to include non-state actors in the policy process. Such changes in the prevailing ideas about security practices challenge the state-centric perspective on international relations and its attendant notion of a distinction between domestic and foreign policy. Consequently, the principles of the Westphalian order are not valid as a starting point for analysing security in the information age. Approaches are required that focus on sub-units of the state, but also take into account specific traits of the international system as changed by the information revolution.

For our purposes, this means that actors and their respective values, interests, and beliefs should be the main unit of research. It is crucial to understand the way individuals adopt changed practices arising from new conceptions of identity and political community, thereby altering interactions among states, or, conversely, the way in which changes in interactions among states lead to changes in practices among individuals (Koslowski and Kratochwil 1996; Braumoeller 2003: 2). Specific actor constellations will develop specific interpretations of information-age security threats and necessary countermeasures. Depending on the “winning” actor constellation and their influence in the policy domain, these interpretations will

dominate the threat debate at given points in time and will be responsible for specific countermeasures.

CONCLUSION

The broad overarching research question addressed in this publication is what the impact of the information revolution is on security and what IR theory can say about these issues. At the beginning of this chapter, a few critical questions were raised concerning this task. We asked ourselves what information security is and how it might be defined in a meaningful way, and came to the conclusion that the term is not precise enough to be useful.

For one thing, many of the anticipated changes seem apparent, but just as many have yet to come into the open, as transformations are ongoing. Statements about the implications of the information revolution on security must be seen in much more relative terms than generally suggested, especially because the outcome of change is truly contradictory and a lot less explicit than some scholars like to envisage. The complexity paradigm further turns one's attention to the concept of the inherently unpredictable situation – a situation that is unpredictable in and of itself, not just by virtue of the limitations of the observer. This resonates well with the general postmodernist approach, in which no objective determination is possible. The new sciences confirm the message that the observer and the observed cannot be detached from each other, and that observation itself is an ontological event. Additionally, the complex is assigned a specific epistemological meaning: It shows the limits of knowledge due to complexity and unpredictability.

Further, if we take the twin-forces of complexity and change seriously, we must reject the notion of a “grand” theoretical project that attempts to distil complexity, paradox, and change into neat theoretical packages and categories. The positivist-empiricist idea, which still dominates the discipline, that a trained observer can encapsulate the amazing complexity of the

world into grand theoretical projects through a variety of rigorous procedures, is antithetic to the current circumstances. While looking at grand theories may have heuristic value, we should acknowledge that everything is in flux and that paradox and uncertainty prevails in today's security environment. This means that even though we might aim to reflect on theoretical premises, any theorizing will be limited in scope, and generalization might be conditional rather than universal.

So, is a theory of the information age needed? All things considered, the information revolution is a very important variable in the equation of the modern world that has the ability to truly change some aspects of international relations. But more importantly, information-age security is not something that can be objectively identified and analysed, but rather an ever-changing construct. What it does, however, is change the perception of security and security practices. To study security in the information age thus means to focus on the process by which key actors subjectively arrive at a shared understanding of what is to be considered and collectively responded to as a security threat in the information age. Even if we conclude that this observation makes a specific theory for information-age security redundant, the forces of the information age are still very poorly understood. Therefore, and due to the fact that there is very little exchange between information-age research and the IR community in general, we believe that the information revolution and its impact on various aspects of IR should continue to be studied in much more depth.

REFERENCES

- Abele-Wigert, I. and Dunn, M. (2006) *The International CIIP Handbook 2006: An Inventory of Protection Policies in 20 Countries and 6 International Organizations* (Vol I), Zurich: Center for Security Studies.
- Albert, A. (1995b) "Chaos and Society: An Introduction", in idem (ed.) *Chaos and Society*, Frontiers in Artificial Intelligence and Applications, vol. 29, Amsterdam: IOS Press, pp. 1-14.
- Albert, A. (ed.) (1995a) *Chaos and Society*, Frontiers in Artificial Intelligence and Applications, vol. 29, Amsterdam: IOS Press.
- Alberts, D. S. and Czerwinski, T. J. (1997) *Complexity, Global Politics, and National Security*, Washington: National Defense University Press.
- Alberts, D. S. and Papp, D. S. (eds.) (1997) *The Information Age: An Anthology of Its Impacts and Consequences, Volume I*, Washington: National Defense University Press.
- Alberts, D. S., Papp, D. S., and Kemp III, W. T (1997) "The Technologies of the Information Revolution", in Alberts, D. S. and Papp, D. S. (eds) *The Information Age: An Anthology of Its Impacts and Consequences, Volume I*, Washington: National Defense University Press.
- Allen, J. H. and Sledge, C. A. (2002) "Information Survivability: Required Shifts in Perspective", *The Journal of Defense Software Engineering*, July, pp. 7-9.
- Ashby, W. R. (1962) "Principles of the Self-organizing System", in von Foerster, H. and Zopf, G. W. (eds.): *Principles of Self-Organization*, New York: Pergamon Press, pp. 255-78.
- Axelrod, R. (1997) *The Complexity of Cooperation: Agent-Based Models of Competition and Collaboration*, Princeton: Princeton University Press.
- Axelrod, R. and Cohen, M.D. (1999) *Harnessing Complexity: Organizational Implications of a Scientific Frontier*, New York: Free Press.
- Baird, Z. (2002) "Governing the Internet: Engaging Government, Business, and Nonprofits", *Foreign Affairs*, 81, 6, pp. 15-20.
- Bak, Per (1996) *How Nature Works: The Science of Self-organized Criticality*, New York: Copernicus.
- Baldwin, D. A. (1997) "The Concept of Security", *Review of International Studies*, 23, 1, pp. 5-28.
- Bar-Yam, Y. (1997) *Dynamics of Complex Systems*, Reading: Addison-Wesley.
- Berkowitz, B. D. (1997) "Warfare in the Information Age", in Arquilla, J. and Ronfeldt, D. (eds) *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica, RAND, pp. 175-90.
- Berkowitz, B. D. (2003) *The New Face of War: How War will Be Fought in the 21st Century*, New York: Free Press.

- Bertalanffy von, L. (1968) *General Systems Theory: Foundations, Development, Applications*, New York: George Braziller Publishing.
- Bertalanffy von, L. (1975) *Perspectives on General System Theory: Scientific-Philosophical Studies*, New York: George Braziller Publishing.
- Biggiero, Lucio (2001) "Sources of Complexity in Human Systems", *Nonlinear Dynamics, Psychology, and Life Sciences*, 5, 1, pp. 3-19.
- Blank, Stephen J. (2003) *Rethinking Asymmetric Threats*, Carlisle: Carlisle Strategic Studies Institute.
- Borgmann, Albert (1999) *Holding on to Reality: The Nature of Information at the Turn of the Millennium*, Chicago: University of Chicago Press.
- Bosch, Olivia (2002) "Cyber Terrorism and Private Sector Efforts for Information Infrastructure Protection", paper presented at the ITU Workshop on Creating Trust in Critical Network Infrastructures, Seoul, 20-22 May 2002.
- Bossomaier, T.R.J. and Green, D.G. (eds.) (2000) *Complex Systems*, Cambridge: Cambridge University Press.
- Bowker, G. (1993) "How to be Universal: Some Cybernetic Strategies 1943-19702", *Social Studies of Science*, 23, 1, pp. 107-28.
- Braumoeller, B.F. (2003) "A Dynamic Solution to the Agent-Structure Debate in International Relations", paper presented at the CEEISA/ISA International Convention, Budapest, Hungary, 26-28 June 2003.
- Butts, C. T. (2001) "The Complexity of Social Networks: Theoretical and Empirical Findings", *Social Networks*, 23, pp. 31-71.
- Buzan, B. and Jones, R. J. B. (eds.) (1981) *Change and the Study of International Relations: The Evaded Dimension*, London: Frances Pinter.
- Byrne, D. (1998) *Complexity Theory and the Social Sciences. An Introduction*, London: Routledge.
- Çambel, A. B. (1992) *Applied Chaos Theory: A Paradigm for Complexity*, Boston: Academic Press.
- Castells, Manuel (1996) *The Rise of the Network Society*, Oxford: Blackwell.
- Casti, J.L. (1979) *Connectivity, Complexity, and Catastrophe in Large-Scale Systems*, Chichester: Wiley and Sons.
- Casti, J.L. (1996) "The Great Ashby", *Journal of Complexity*, 2, 1, pp. 7-9.
- Cederman, L-E. (1997) *Emergent Actors: How States and Nations Develop and Dissolve*, Princeton: Princeton University Press.

- Cederman, L-E. and Gleditsch, K.S. (2004) "Conquest and Regime Change: An Evolutionary Model of the Spread of Democracy and Peace", *International Studies Quarterly*, 48, 3, pp. 603-29.
- Cohen, E. (1996) "A Revolution in Military Affairs", *Foreign Affairs*, 75, 2, pp. 37-54.
- Cohen, R.S. (1995) "How Useful Is the Complexity Paradigm Without Quantifiable Data? A Test Case: The Patronage of 5th-6th Century Buddhist Caves in India", in Albert, A. (ed.) *Chaos and Society*, Frontiers in Artificial Intelligence and Applications, vol. 29, Amsterdam: IOS Press, pp. 83-99.
- Cooper, J.R. (1997) "Another View of the Revolution in Military Affairs, in Arquilla, J. and Ronfeldt, D. (eds) *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica: RAND, pp. 99-140.
- Crutchfield, J. P. (1994) 'Is Anything Ever New? Considering Emergence', in Cowan, G., Pines, D. and Melzner, D. (eds) *Complexity: Metaphors, Models, and Reality*, SFI Series in the Sciences of Complexity XIX, Redwood City: Addison-Wesley, pp. 479-97.
- Crutchfield, James P., Farmer, J. P., Packard, N. H. and Shaw, R. S. (1986) "Chaos", *Scientific American*, December, pp. 46-57.
- CSIS, Center for Strategic and International Studies (1996) *The Information Revolution and International Security: Robert F. McCormick Tribune Foundation Report*, Washington: Center for Strategic and International Studies.
- David, N.C. (1997) "An Information-Based Revolution in Military Affairs", in Arquilla, J. and Ronfeldt, D. (eds) *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica: RAND, pp. 79-98.
- Deibert, Ronald J. (1997) *Parchment, Printing, and Hypermedia: Communication in World Order Transformation*, New York: Columbia University Press.
- Devost, M.G., Houghton, B.K. and Pollard, N.A. (1997) "Information Terrorism: Political Violence in the Information Age", *Terrorism and Political Violence*, 9, 1, pp. 72-83.
- Downes, L., Mui, C. and Negroponete, N. (1998) *Unleashing the Killer App: Digital Strategies for Market Dominance*, Cambridge, MA: Harvard Business School Press.
- Dunn, M. (2002) *Information Age Conflicts: A Study on the Information Revolution and a Changing Operating Environment*, Zürcher Beiträge zur Sicherheitspolitik und Konfliktforschung, No. 64, Zurich: Center for Security Studies.
- Dunn, M. (2005) "The Socio-Political Dimensions of Critical Information Infrastructure Protection (CIIP)", *International Journal for Critical Infrastructure Protection*, 1, 2/3, pp. 58-68.
- Dunn, M. (2006) "Understanding Critical Information Infrastructures: An Elusive Quest", in: Dunn, M. and Mauer, V. (eds.) *The International CIIP Handbook 2006: Analyzing Issues, Challenges, and Prospects* (Vol. II), Zürich, Forschungsstelle für Sicherheitspolitik, pp. 27-53.

- Dunn, M. and Wigert, I. (2004) *The International CIIP Handbook 2004: An Inventory of Protection Policies in Fourteen Countries*, Zurich: Center for Security Studies.
- Eriksson, J. (2001b) "Cyberplagues, IT, and Security: Threat Politics in the Information Age", *Journal of Contingencies and Crisis Management*, 9, 4, pp. 211-22.
- Eriksson, J. (ed.) (2001a) *Threat Politics: New Perspectives on Security, Risk and Crisis Management*, Ashgate: Aldershot.
- Eve, R. A., Horsfall, S. and Lee, M. E. (eds) (1997) *Chaos, Complexity, and Sociology: Myths, Models, and Theories*, Thousand Oaks: Sage Publications.
- Foerster von, H. and Zopf, G.W. (eds.) (1962) *Principles of Self-Organization*, New York: Pergamon Press.
- Forrester, J. W. (1961) *Industrial Dynamics*, Massachusetts: Productivity Press.
- Freeman, C. and Louca, F. (2002) *As Time Goes By: From the Industrial Revolutions to the Information Revolution*, Oxford, Oxford University Press.
- Gleick, J. (1987) *Chaos: Making a New Science*, New York: Penguin Books.
- Gomez, P. (2001) „Vom Umgang mit Komplexität: Denkfallen und Entscheidungshilfen“, in Mey, H. and Lehmann Pollheimer, D., *Absturz im freien Fall – Anlauf zu neuen Höhenflügen: Gutes Entscheiden in Wirtschaft, Politik und Gesellschaft*, Zürich: Vdf Hochschulverlag AG, pp. 151-66.
- Goodman, S.E., Hassebroek, P.B., King, D. and Azment, A. (2002) *International Coordination to Increase the Security of Critical Network Infrastructures*, Document CNI/04, paper presented at the ITU Workshop on Creating Trust in Critical Network Infrastructures, Seoul, 20-22 May 2002.
- Hobart, M.E. and Schiffman, Z.S. (2000) *Information Ages: Literacy, Numeracy, and the Computer Revolution*, Washington: Johns Hopkins University Press.
- Holsti, K.J. (1998) "The Problem of Change in International Relations Theory", Institute of International Relations, The University of British Columbia, Working Paper No. 26, December.
- Husain, Khurram Neocons (2003) "The Men Behind the Curtain", *Bulletin of the Atomic Scientists*, 59, 6, pp. 62-71.
- Jervis, Robert (1997b) „Complex Systems: The Role of Interactions“, in Alberts, D.S. and Czerwinski, T.J. (eds) *Complexity, Global Politics, and National Security*, Washington: National Defense University Press, pp. 45-71.
- Jervis, Robert (1997a) *System Effects: Complexity in Political and Social Life*, Princeton: Princeton University Press.
- Kellert, Stephen H. (1995) "When is the Economy Not Like the Weather? The Problem of Extending Chaos Theory to the Social Sciences", in Albert, A. (ed.) *Chaos and Society. Frontiers in Artificial Intelligence and Applications*, vol. 29, Amsterdam: IOS Press, pp. 35-48.

- Keohane, R.O. and Nye, J.S. (1977) *Power and Interdependence: World Politics in Transition*, Boston, Little Brown and Company.
- Keohane, R.O. and Nye, J.S. (1998) "Power and Interdependence in the Information Age", *Foreign Affairs* 77, 5 (September/October): pp. 81-94.
- Kolet, K.S. (2001) "Asymmetric Threats to the United States", *Comparative Strategy*, 20, 3, pp. 277-92.
- Koslowski, R. and Kratochwil, F.V. (1996) "Understanding Change in International Politics: The Soviet Empire's Demise and the International System", in: Lebow, R.N. and Risse-Kappen, T. (eds.) *International Relations Theory and the End of the Cold War*, New York: Columbia University Press.
- Kratochwil, F. (1989) *Rules, Norms and Decisions: On the Conditions of Practical and Legal Reasoning in International and Domestic Affairs*, Cambridge: Cambridge University Press.
- Kyriakopoulos, N. and Wilikens, M. (2000) *Dependability and Complexity: Exploring Ideas for Studying Open Systems*, Ispra: Joint Research Centre.
- Laszlo, E. (1991) *The Age of Bifurcation: Understanding the Changing World*. The World Futures General Evolution Studies, Volume 3, Philadelphia (etc.): Gordon and Breach.
- Lewis, J.A. (2002) *Assessing the Risks of Cyber-terrorism, Cyber War and Other Cyber Threats*, Washington: Center for Strategic and International Studies.
- Libicki, M. (1995) *What is Information Warfare?* Washington, DC, National Defense University.
- Libicki, Martin (1999) *Illuminating Tomorrow's War*, Mc Nair Paper 61, Washington, DC, National Defense University.
- Luijff, E.A.M., Burger, H.H. and Klaver, M.H.A (2003) "Critical Infrastructure Protection in The Netherlands: A Quick-scan", in: Gattiker, U.E., Pedersen, P. and Petersen, K. (eds.). *EICAR Conference Best Paper Proceedings 2003*, Copenhagen, Denmark.
- Masera, M. and Wilikens, M. (2001) "Interdependencies with the Information Infrastructure: Dependability and Complexity Issues", paper given at the 5th International Conference on Technology, Policy, and Innovation, Ispra, June 26-29, 2001.
- Merry, U. (1995) *Coping with Uncertainty: Insights from the New Sciences of Chaos, Self-organization, and Complexity*, Westport: Praeger.
- Metcalf, B. (1995) "Metcalf's Law: A network becomes more valuable as it reaches more users", *Infoworld* October 2, 1995: p. 53.
- Metz, S. and Johnson, D.V. (2001) *Asymmetry and U.S. Military Strategy: Definition, Background, and Strategic Concepts*, Carlisle: Strategic Studies Institute.
- Michaels, Mark (1995) "Seven Fundamentals of Complexity for Social Science Research", in Albert, A. (ed.) *Chaos and Society*. Frontiers in Artificial Intelligence and Applications, vol. 29., Amsterdam: IOS Press, pp. 15-34.

- Mihata, K. (1997) "The Persistence of 'Emergence'", in Eve, R.A., Horsfall, S. and Lee, M.E. (eds) *Chaos, Complexity, and Sociology: Myths, Models, and Theories*, Thousand Oaks: Sage Publications, pp. 30-38.
- Moore, G. E. (1965) "Cramming More Components onto Integrated Circuits", *Electronics*, 38, 8, pp. 114-17.
- Moteff, J.D. (2003) *Critical Infrastructures: Background, Policy, and Implementation*, Congressional Research Report for Congress, RL30153, 10 February 2003, Washington, DC: Congressional Research Service.
- Moteff, J.D., Copeland, C. and Fischer, J. (2002) *Critical Infrastructures: What Makes an Infrastructure Critical?* Congressional Research Report for Congress, RL31556, 29 January 2002, Washington, DC: Congressional Research Service.
- Nichiporuk, B. and Builder, C.H. (1997) "Societal Implications", in Arquilla, J. and Ronfeldt, D. (eds) *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica, RAND, pp. 295-314.
- Nye, J.S. (1990) "Soft Power", *Foreign Policy*, 80, pp. 153-71.
- Nye, J.S. (1998) "U.S. Security Policy: Challenges for the 21st Century", *USIA Electronic Journal*, 3, 3.
- Nye, J.S. and Owens, W.A. (1996) "America's Information Edge", *Foreign Affairs* (March/April): pp. 20-36.
- O'Brien, K.A., Ligtoet, A., Rathmell, A. and MacKenzie, D. (2003). *Using Scenarios to Support Critical Infrastructure Analysis and Assessment Work*. ACIP, Package 3 Deliverable D3.4.
- OCIPEP (2003) Office of Critical Infrastructure Protection and Emergency Preparedness, "Threats to Canada's Critical Infrastructure", Threat Analysis TA03-001, 12 March 2003.
- Papp, D.S. and Alberts, D.S. (1997) "The Impacts of the Information Age on International Actors and the International System", in Alberts, D.S. and Papp, D.S. (eds) *The Information Age: An Anthology of Its Impacts and Consequences*, Washington, DC: National Defense University.
- Papp, D.S., Alberts, D.S. and Tuyahov, A. (1997) "Historical Impacts of Information Technologies: An Overview", in Alberts, D.S. and Papp, D.S. (eds) *The Information Age: An Anthology of Its Impacts and Consequences*, Washington, DC, National Defense University.
- Parker, D.B. (1983) *Fighting Computer Crime*, New York: Charles Scribner's Sons.
- Perrow, C. (1984) *Normal Accidents: Living with High-Risk Technologies*, New York: Basic Books.
- Pollitt, M.M. (1997) "Cyberterrorism – Fact or Fancy?", *Proceedings of the 20th National Information Systems Security Conference*, 1997, pp. 285-89.

- Prigogine, I. (1981) *From Being to Becoming: Time and Complexity in the Physical Sciences*, San Francisco: W H Freeman & Co.
- Rathmell, A. (2001) "Controlling Computer Network Operations", *Information & Security: An International Journal*, 7, pp. 121-44.
- Rinaldi, S.M., Peerenboom, J.P. and Kelly, T.K (2001) "Complex Networks. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies", *IEEE Control Systems Magazine*, 21, 6 (December): pp. 11-25.
- Rosecrance, R. (1999) *The Rise of the Virtual State. Wealth and Power in the Coming Century*, New York: Basic Books.
- Rosenau, J. (1997) "Many Damn Things Simultaneously: Complexity Theory and World Affairs", in Alberts, D.S. and Czerwinski, T.J (eds.) *Complexity, Global Politics, and National Security*, Washington, DC: National Defense University Press, pp. 73-100.
- Rosenau, J.N. (1990) *Turbulence in World Politics: A Theory of Change and Continuity*, Princeton: Princeton University Press.
- Rosenau, J.N. (1992) "Governance, Order, and Change in World Politics", in Rosenau, J.N. and Czempiel, E.-O. (eds.) *Governance Without Government: Order and Change in World Politics*, Cambridge Studies in International Relations Nr. 20, Cambridge: Cambridge University Press, pp.1-29.
- Rosenau, J.N. (1998) "Global Affairs in an Epochal Transformation", in Henry, C. R. and Peartree, E.C. (eds) *Information Revolution and International Security*, Washington, DC: Center for Strategic and International Studies, pp. 33-57.
- Rothkopf, D.J (1998) "Cyberpolitik: The Changing Nature of Power in the Information Age", *Journal of International Affairs* 51, 2 (Spring): pp. 325-60.
- Ruggie, J. (1993) "Territoriality and Beyond: Problematizing Modernity in International Relations", *International Organization* 47, 4, pp.140-74.
- Shannon, C. and Weaver, W. (1949) *The Mathematical Theory of Communications*, Urbana: University of Illinois Press.
- Strange, S. (1988) *State and Markets: An Introduction to International Political Economy*, New York: Basil Blackwell, pp. 25-31.
- Turner, B.A. and Pidgeon, N.F. (1997²) *Man-Made Disasters*, Oxford: Butterworth-Heinemann.
- Turner, F. (1997) "Foreword", in Eve, R.A., Horsfall, S. and Lee, M.E. (eds) *Chaos, Complexity, and Sociology: Myths, Models, and Theories*, Thousand Oaks: Sage Publications, pp. xi-xxvii.
- Waldrop, M.M. (1992) *Complexity: The Emerging Science at the Edge of Order and Chaos*, New York: Simon and Schuster.

- Waldrop, M.M. (1998) "Is There an Information Revolution?", in Henry, C.R. and Peartree, E.C. (eds) *Information Revolution and International Security*, Washington, DC, Center for Strategic and International Studies Press, pp. 1-9.
- Wolfers, A.(1962) "National Security as an Ambiguous Symbol", in idem (ed.) *Discord And Collaboration: Essays on International Politics*, Baltimore: Johns Hopkins, pp. 147-65.
- Zacher, M.W. (1992) "The Decaying Pillars of the Westphalian Temple: Implications for International Order and Governance", in Rosenau, J.N. and Czempiel, E.-O., *Governance Without Government: Order and Change in World Politics*, Cambridge Studies in International Relations Nr. 20, Cambridge: Cambridge University Press, pp. 58-101.