THE INTERNET AND THE CHANGING FACE OF INTERNATIONAL RELATIONS AND SECURITY

Andreas WENGER

Most experts agree today, at the beginning of the 21st century, that we are experiencing a period of fundamental change. Understandably, there is much uncertainty about what kind of world the current global transformations will produce. In order to understand these changes and adapt to them we need to develop new conceptual repertoires that will better equip us to meet the challenges posed by the speed with which the world is evolving and the extreme global complexity that is emerging. One factor that is helping to create this new environment is information technology and, most significantly, the Internet. To fully comprehend the Internet's impact on how we think about and practice international relations and security, we need to investigate the conventional approaches that have inspired practitioners and theoreticians until now.

Since its inception, the discipline of international relations (IR) has been based on a separation between internal and external state relations. This separation was bequeathed to the modern state system by the Treaty of Westphalia in 1648, which attempted to resolve the religious conflicts of the Thirty Years' War by replacing a universal religious authority who acted as the arbiter of Christendom with the state-sovereign within its own territory and with the right to non-intervention in its affairs by any other state. After 1648, the internal affairs of states were thus conceptually separated from the external arena of interstate relations. At the beginning of the 21st century, however, we have reached a point where the traditional *domestic-international* framework no longer holds.

The division between affairs internal and foreign affairs is becoming increasingly untenable in an environment where international politics are more and more driven by the forces of *globalization* and *localization*. The information technology revolution has dramatically accelerated the cross-border movement of goods, services, ideas, and capital, resulting in a huge increase in transnational cultural and political exchanges and in the emergence of many new institutions and structures that

transcend state borders. Modern information technologies have minimized the previous limitations imposed by space and time on the mobility of worldwide capital and industry and have created an environment for global trade and investment decisions. At the same time, local factors like workforce skills, hard and soft infrastructure, legal norms, and political institutions allow local communities and actors to attract mobile capital, human resources, business deals, and multinational firms. The resulting complex web of relations simply cannot be characterized as either domestic or international. The key political challenge now is to strike the right balance between international and local forces.

Although there is widespread belief that the information technology revolution is restructuring the international system, there is far less consensus about the theoretical and practical impact of the often contradictory developments on international politics. Given that the world is experiencing a diffusion of territorial, societal, and economic space, the debate initially centered on the redistribution and the changing nature of power. The distribution of power has become increasingly volatile and complex, and traditional political and cultural boundaries that once defined distinct worlds are beginning to crumble. The transnational architecture of global information networks has made territorial borders less significant. War and peace in the information age are evolving in an environment in which the boundaries between the political space and the military space have become increasingly blurred, as have those between the civilian domain and the military domain.

Power in the global information society depends less on territory, military power, and natural resources. Rather, information, technology, and institutional flexibility have gained in importance in international relations. In an unpredictable and highly turbulent international environment, the soft powers of knowledge, beliefs, and ideas allow political actors to achieve their goals. Opposing powers these days are less inclined to battle out their differences in the physical arena. Rather, they focus on the information domain, and gaining access to information is now the central strategic principle. Networks wage wars, and small players can now outsmart huge opponents by using asymmetrical strategies. However, our understanding of such conflicts and their multifaceted dynamics remains limited at best.

The importance of information and knowledge today is forcing us to take a new look at the main actors in international relations. Traditionally, states have been the exclusive holders of power and authority. However, with the advent of the Internet, new and diverse actors have entered the stage, and simultaneously the speed, capacity, and flexibility in the collection, production, and dissemination of information have increased. As decentralized network-based soft power structures have gained in importance, 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. These new contenders rely on the power to persuade a public that is increasingly global, and they are now able to mobilize support for an array of issues, with both good and bad intentions. The huge increase in the number of actors and the potential fluidity of the international political agenda complicate considerably the conduct of statecraft and the formulation of foreign policy.

As a result of the fragmentation of authority and the altered quality of power, the traditional foundations of security have also been turned upside down. The object of security is no longer simply the territorial integrity of the state. The information revolution has dramatically increased the dependence of developed countries on efficient national and transnational information infrastructures. Modern information technologies have brought about new vulnerabilities and risks. In developed societies key critical infrastructures—electricity production and distribution, transportation, financial services, telecommunications, and the water supply—are reliant on information systems and are highly vulnerable. Threats to these structures are less likely to come from so-called rogue states than from hostile non-state actors, such as international terrorists or cyber criminals operating in a relatively opaque cyberspace that has yet to be subjected to effective regulation.

Clearly, the state is not the only international actor that provides public services such as security, welfare, education, and law. The developments of the past decade have led many observers to assume that the forces driving global change are undermining the state and its political agency. However, we are not witnessing the end of the nation state but a return to overlapping authorities. Clearly, the state has to adapt its functions to the conditions of a rapidly changing international environment. Although the growing importance of soft power presents new challenges to the state's traditional monopoly of authority, states still possess sufficient agency to influence the extra-territorial realm of action that the Internet has helped to create. Indeed, the past few years show a clear tendency towards a centralization of power, and states are increasingly acting in this extra-territorial space and are "internationalizing" some of their functions. We believe, therefore, that there is no reason to assume that the Internet is undermining the power of the state and that there is every reason to expect that states will collectively enforce their sovereignty in cyberspace.

The extent to which individual states will meet the challenge of an expanded and highly unpredictable domain of action will vary, not least because of the so-called digital divide. States will have to address potential threats to security that will likely emerge as a result of an unequal distribution of soft power. Countries, regions, and various groups already suffering economic hardship and political and cultural alienation are unlikely to feel the benefits of soft power. Thus, while developed states may be tempted to exploit the opportunities afforded to them by information

technologies in order to gain advantages over their rivals, they will have to weigh this against the cost of ignoring their vulnerability to asymmetrical threats. A reduction of security risks will not only entail increased multilateral cooperation but also increased engagement with non-state actors—most notably those in the private sector who own information systems—and with people, states, and regions that already feel marginalized.

The relationship between the Internet and modern international relations is a broad and multifaceted topic. In the present publication we have assembled a series of articles that provide an overview of the scope and complexities of this area of inquiry.

The Growth of Soft Power and the Challenges of Global Governance

The first three articles deal with the broad challenges to governance posed by the growth of soft power. The first, by Giacomello and Mendez, explores the impact of the Internet on state sovereignty. The authors take issue with the widespread presupposition that the Internet entails a diminution of state sovereignty and of the state's importance as an actor. They analyze four areas in which the Internet has affected a shift in state sovereignty: ICANN, the French Yahoo!-court case, taxation on the Internet, and cyber crime. The authors conclude that although the Internet poses new challenges to conventional state authority, the state generally remains the prime negotiator of globalization and of the Internet.

The article by Brown and Studemeister focuses on the effect the Internet has had on the state practice of diplomacy. The authors claim that the empowerment afforded by networks means that states are now required to engage with a variety of non-state actors—influential multinationals, temporary and diverse coalitions, networks of citizens with various allegiances, and other non-state actors—on issues that are increasingly perceived as global and interdependent. The authors examine several recent reports produced by the US foreign affairs establishment and conclude that Washington is heeding the call to bring diplomacy in line with today's complex and increasingly global environment.

In the third article Zinnbauer addresses the uneven distribution of soft power around the globe. The author focuses specifically on the implications of the digital divide with regard to global governance decision-making. He argues that any attempts to frame the problem in terms of resource and/or skill inequalities are misguided and lead too easily to the conclusion that the participation by grass-roots groups in global governance decision-making is a merely technical issue. The author claims that the biggest obstacle to representation in global governance is the political situation in some developing countries, not the digital divide per se. Here, he suggests, new information and communication technologies can enable grass-roots participation in

issues of global governance, for example by allowing information and communication to flow from grass-roots groups to the community and from there to international advocacy groups. The author concludes that the plurality of voices in global governance decision-making depends on a mixture of old and new gatekeepers.

The New Security Challenges of the Information Age

The second set of articles deals with the security challenges posed by the Internet. The first article, by Westrin, examines some fundamental issues related to the protection of critical information infrastructures. The article looks at what or who should be secured, how security should be achieved, and where the responsibility for security will ultimately lie. The author argues that societal information infrastructures constitute an important new object of security. The article outlines the basic differences between conventional and IT-related security threats and discusses the various difficulties involved in appreciating the vulnerabilities and securing a fragmented and continually evolving resource. The article concludes with a short description of the state of critical information infrastructure protection (CIIP) research.

The next article, by Bendrath, centers on the information society as a risk society. The author stresses the novel characteristics of cyber risks: the new weapons are not kinetic but are software and knowledge; the environments in which attacks occur are not physical, but virtual; and the attacker is unknown and can hide during an attack. The author then goes on to explore the US policy response to the risk of cyber attacks on critical information infrastructures. Bendrath shows that although IT-security threats were initially framed in military terms, either as cyberwar or information warfare, the emphasis later shifted, bringing about the need to encourage law enforcement involvement, public-private sector partnership, and public and private self-help strategies. Three factors are identified as responsible for this shift of direction: differences between risk perception in law enforcement and in the private sectors; the private control of technical resources; and the constraining effect of cultural and legal norms.

The aim of the third article in this group, by Näf, is to increase awareness of the vulnerabilities of our information systems. The author does this by explaining several techniques currently used by computer hackers. The article also highlights several insecure aspects of present critical societal infrastructure, suggests some security-related developments, and makes recommendations for improving the security of information systems.

The Human Mind as Battlefield in an Emerging Global Information Environment

The remaining articles are concerned with problems arising from the dual use quality of information systems and the need to regulate the use with bad intent. The first article, by Rathmell, explores the viability of an international regime for controlling computer network operations (CNOs), defined by him as malicious computer-mediated activities. The author identifies a strategic dilemma: States are keen to exploit CNOs to gain an advantage in the military sphere, yet they also need to protect the global information environment on which so many societies depend. Underlying the dilemma are two significantly different ways in which states can understand the policy challenge that CNOs present them with: On the one hand, they might focus their policy on the interdependencies created by network-based power, which in turn have created a need for cooperation in order to ensure trust in and the survival of information systems; on the other hand, they might focus their policy on the strategic advantage that CNOs offer as a new form of weapon in an essentially anarchic environment. The author discerns a decrease in importance of the latter approach in the 1990s and a new emphasis on cooperation between the private sector and government agencies. Yet there is a schism, at the multilateral level, between NATO and the EU: While NATO is seeking to legitimize and make routine use of CNOs, the EU is seeking to de-legitimize cyber attacks and to build robust global information networks. Rathmell concludes that military thinking on CNOs, like that underpinning NATO's position, misses important truths about the emergent global information environment and is responsible for blocking progress in developing IT-related security regimes.

The second article, by Dunn, explores the growing importance of the Internet in conflict situations. The author discusses the new conflict environment, in which there is a proliferation of voices, and where intelligence gathering, dissemination of information, and mobilization of support are carried out over the Internet. The human mind is thus a prime target on today's battlefields. The article concludes that information attacks are likely to set precedents in approaches to CNOs, the use of the Internet as a tool of war, and international law. Dunn reminds us that we need to ensure that civilians are not made targets, either in the struggle for hearts and minds or through a possible targeting of civilian installations.

The last article, by Thomas, examines three aspects of civilian and military use of the Internet in China. The author first explores the rapid growth in Internet use by civilians, the information technologies that support the Internet, and the role of Jiang Zemin's son in the information technology revolution. He also explores the integration of the Internet into military operations, both as a means of mobilizing the emotions of People's Liberation Army and of providing news. Finally, the article

investigates three recent Internet skirmishes in which Chinese citizens have been involved, namely against NATO in April and May of 1999, against Taiwan in August and September of 1999, and against the United States in April of 2001. The author concludes that these are dangerous precedents in cyberspace, where regulation is clearly lacking.

ACKNOWLEDGEMENT. The editor would like to thank Myriam Dunn for her support and enthusiasm for the project. She has always offered her assistance gladly and never failed to be there to see the project through to completion. Special thanks go to Lisa Watanabe, Christopher Findlay, and Michelle Norgate for their invaluable help with the manuscript.

ANDREAS WENGER is professor of international security policy and deputy director of the Center for Security Studies and Conflict Research (www.fsk.ethz.ch) at the Swiss Federal Institute of Technology Zurich (ETH). He has worked extensively in the area of security and strategic studies; US, Russian, and Swiss foreign and security policy; transatlantic relations; and Cold War and international history. His publications include *Living with Peril: Eisenhower, Kennedy, and Nuclear Weapons* (Lanham: Rowman & Littlefield Publishers, 1997), *Russia's Place in Europe: A Security Debate* (Bern: Peter Lang, 1999), and *Nuclear Weapons into the 21st Century: Current Trends and Future Prospects* (Bern: Peter Lang, 2001). He is also the author of a number of articles in scholarly journals and collections of scholarly works. Professor Wenger manages the International Relations and Security Network ISN (www.isn.ethz.ch), a leading knowledge management platform on the Internet in the fields of international relations and security. Within the ISN, he is involved in the Integrated Risk Analysis and the Critical Information Infrastructure Protection projects (www.isn.ethz.ch/crn/index.cfm). *E-mail*: wenger@sipo.gess.ethz.ch.