out of the reach of those states whose laws they have violated and whose populations provide customers for their illicit products and services.

There is another possible consequence that is even more disturbing: it is not inconceivable that the major global divide will be caused not by competing ideologies, the struggle for power, or Huntington's "clash of civilizations," but by clashes between states that uphold law and order and those that are dominated by criminal interests and criminal authorities.

NOTES

1. James Rosenau, *Turbulence in World Politics* (Princeton, N.J.: Princeton University Press, 1990).
2. Diego Gambetta, *The Sicilian Mafia: The Business of Private Protection* (Cambridge, Mass.: Harvard University Press, 1993).
3. Francisco E. Thoumi, *Political Economy and Illegal Drugs in Colombia* (Boulder, Colo.: Lynne Rienner, 1995), pp. 172–73.
4. Roy Godson, "Political–Criminal Nexus: Overview," *Trends in Organized Crime*, 3 (1) (Fall 1997), 4–7.
5. Charles Tilly, "War Making and State Making as Organized Crime," in Peter B. Evans, Dietrich Rueschemeyer, and Theda Skocpol (eds.), *Bringing the State Back In* (Cambridge: Cambridge University Press, 1985), pp. 169–91.

Cyber Conflict and National Security[1]

HERBERT LIN

WHAT IS CYBERSPACE AND WHY IS IT IMPORTANT

In the 21st century, information is the key coin of the realm, and thus entities from nation-states to individuals are increasingly dependent on information and information technology (to include both computer and communications technologies). Businesses rely on information technology (IT) to conduct operations (e.g., payroll and accounting, recording inventory and sales, research and development (R&D). Distribution networks for food, water, and energy rely in IT at every stage, as do transportation, health care, and financial services. Factories use computer-controlled machinery to manufacture products more rapidly and more efficiently than ever before.

Military forces are no exception. IT is used to manage military forces (e.g., for command and control and for logistics). The use of IT embedded in modern weapons systems increases the lethality and reduces the collateral damage

[1] Herbert Lin, "Cyber Conflict and National Security." Reprinted by permission of Herbert Lin.

associated with the use of such weapons. Movements and actions of military forces can be coordinated through networks that allow information and common pictures of the battlefield to be shared widely.

Terrorists also use IT. Although the kinetic weapons of terrorists are generally low-tech, terrorist use of IT for recruitment, training, and communications is often highly sophisticated.

WHAT IS CONFLICT IN CYBERSPACE?

Given the increasing importance of information and IT, it is not surprising that parties might seek to gain advantage over their adversaries by using various tools and techniques for taking advantage of certain aspects of cyberspace—what this paper will call "conflict in cyberspace" or "cyber conflict."[2]

Tools/Techniques

The tools and techniques of conflict in cyberspace can be usefully separated into tools based on technology and techniques that focus on the human being. Offensive tools and techniques allow a hostile party to do something undesirable. Defensive tools and techniques seek to prevent a hostile party from doing so.

Technology-based Tools An offensive tool requires three components:

- Access refers to how the hostile party gets at the IT of interest. Access may be remote (e.g., through the Internet, through a dial-up modem attached to it, through penetration of the wireless network to which it is connected). Alternatively, access may require close physical proximity (e.g., spies acting or serving as operators, service technicians, or vendors). Close access is a possibility anywhere in the supply chain (e.g., during chip fabrication, assembly, loading of system software, during shipping to the customer, during operation).
- A vulnerability is an aspect of the IT that can be used to compromise it. Vulnerabilities may be accidentally introduced through a design or implementation flaw, or introduced intentionally (see close-access above). An unintentionally introduced defect ("bug") may open the door for opportunistic use of the vulnerability by an adversary.
- Payload is the term used to describe the mechanism for affecting the IT after access has been used to take advantage of a vulnerability. For example, once a software agent (such as a virus) has entered a computer, its payload can be programmed to do many things—reproducing and retransmitting itself, destroying files on the system, altering files. Payloads can be designed to do more than one thing, or to act at different times. If a communications channel is available, payloads can be remotely updated.

Defensive tools address one or more of these elements. For example, some tools (e.g., firewalls) close off routes of access that might be inadvertently left

open. Other tools identify programming errors (vulnerabilities) that can be fixed before a hostile party can use them. Still others serve to prevent a hostile party from doing bad things with any given payload (e.g., a confidential file may be encrypted so that even if a copy is removed from the system, it is useless to the hostile party).

People-based Techniques People interact with information technology, and it is often easier to trick, bribe, or blackmail an insider into doing the bidding of a hostile party. For example, close access to a system may be obtained by bribing a janitor to insert a USB flash drive into a computer. A vulnerability may be installed by blackmailing a programmer into writing defective code. Note that in such cases, technical tools and people-based techniques can be combined.

Defensive people-based techniques essentially involve inducing people to not behave in ways that compromise security. Education teaches (some) people not to fall for scams that are intended to obtain log-in names and passwords. Audits of activity persuade (some) people not to use IT in ways that are suspicious. Rewards for reporting persuade (some) people to report questionable or suspicious activity to the proper authorities.

Possible Offensive Operations in Cyberspace

Offensive activity in cyberspace can be described as cyberattack or cyber exploitation.

- Cyberattack refers to the use of deliberate activities to alter, disrupt, deceive, degrade, or destroy computer systems or networks used by an adversary or the information and/or programs resident in or transiting these systems or networks. The activities may also affect entities connected to these systems and networks. A cyberattack might be conducted to prevent authorized users from accessing a computer or information service (a denial of service attack), to destroy computer controlled machinery (the alleged purpose of the Stuxnet cyberattack[3]), or to destroy or alter critical data (e.g., timetables for the deployment of military logistics). Note that the direct effects of a cyberattack (damage to a computer) may be less significant than the indirect effects (damage to a system connected to the computer).
- Cyber exploitation refers to deliberate activities to penetrate computer systems or networks used by an adversary for obtaining information resident on or transiting through these systems or networks. Cyberexploitations do not seek to disturb the normal functioning of a computer system or network from the user's point of view—indeed, the best cyberexploitation is one that such a user never notices. The information sought is generally information that the adversary wishes not to be disclosed. A nation might conduct cyber exploitations to gather for valuable intelligence information, just as it might deploy human spies to do so. It might

seek information on an adversary's R&D program for producing nuclear weapons, or on the adversary's order of battle, its military operational plans, and so on. Or it might seek information from a company's network in another country in order to benefit a domestic competitor of that company. Of particular interest is information that will allow it to conduct further penetrations on other systems and networks to gather additional information.

Note that press accounts often refer to cyberattacks when the activity conducted is a cyber exploitation.

Actors/Participants and Their Motivations

What actors might conduct such operations? The nature of information technology is such that the range of actors who can conduct operations of national-level significance is potentially large. Certain nation states, such as the United States, China, Russia, and Israel, are widely regarded as having potent offensive cyber capabilities, although smaller nation states can also conduct offensive operations in cyberspace.

To date, the known actors who have perpetrated acts of cyber exploitation and cyberattack are subnational parties—mostly individuals and mostly for profit. It is often alleged that Russia was behind the cyberattacks against Estonia in 2007 and Georgia in 2008, that China is behind a number of high-profile cyber exploitations against entities in many nations, and that the United States and/or Israel were responsible for the cyberattack on Iranian nuclear facilities (Stuxnet); however, none of these nations have officially acknowledged undertaking any of these activities, and conclusive proof, if any, that the political leadership of any nation ordered or directed any of these activities has not been made public.

A variety of subnational actors—including individuals, organized crime, and terrorists—might conduct cyberattacks and/or cyber exploitations. Indeed, some (but only some) such operations can be conducted with information and software found on the Internet and hardware available at Best Buy or Amazon.

Motivations for conducting such operations also span a wide range. One of the most common reasons today is financial. Because a great deal of commerce is enabled through the Internet or using IT, some parties are cyber criminals who seek illicit financial gain through their offensive actions. Cyber exploitations can yield valuable information, such as credit card numbers or bank log-in credentials; trade secrets; business development plans; or contract negotiation strategies. Cyberattacks can disrupt the production schedules of competitors, destroy valuable data belonging to a competitor, or be used as a tool to extort money from a victim. Perpetrators might conduct a cyberattack for hire (it is widely believed that the cyberattack on Estonia was conducted using a rented cyber weapon).

Another possible reason for such operations is political—the perpetrator might conduct the operation to advance some political purpose. A cyberattack

or exploitation may be conducted to send a political message to a nation, to gather intelligence for national purposes, to persuade or influence another party to behave in a certain manner, or to dissuade another party from taking certain actions.

Still another reason for conducting such operations is personal—the perpetrator might conduct the operation to obtain "bragging rights," to demonstrate mastery of certain technical skills, or to satisfy personal curiosities.

Lastly, such operations may be conducted for military reasons, in the same way that traditional military operations involving kinetic weapons are used. This point is discussed below.

HOW CONFLICT IN CYBERSPACE COMPARES TO CONFLICT IN PHYSICAL SPACE

Much about cyber conflict upends our understanding of how conflict might unfold. Although most observers would acknowledge clear differences between the cyber domain and physical domains, it is easy to underestimate just how far-reaching these differences are. Consider, for example, the impact of:

- Venue for conflict. In traditional kinetic conflict (TKC), military activities occur in a space that is largely separate from the space in which large numbers of civilians are found. In cyber conflict, the space in which many military activities occur is one in which civilians are ubiquitous.
- The offense-defense balance. In TKC, offensive technologies and defensive technologies are often in rough balance. In cyber conflict (at least prior to the outbreak of overt hostilities), the offense is inherently superior to the defense, because the offense needs to be successful only once, whereas the defense needs to succeed every time.
- Attribution. TKC is conducted by military forces that are presumed to be under the control of national governments. No such presumptions govern the actors participating in cyber conflict, and definitive attribution of acts in cyberspace to national governments is very difficult or impossible (see discussion below).
- Capabilities of non-state actors. In TKC, the effects that non-state actors can produce are relatively small compared to those that can be produced by state actors. In cyber conflict, non-state actors can produce some of the large-scale effects that large-scale actors can produce.
- The importance of distance and national borders. In TKC, distance looms large, and violations of national borders are significant. In cyber conflict, distance is more or less irrelevant, and penetrations of national boundaries for both attack and exploitation occur routinely and without notice.

These differences have pervasive effects on how to conceptualize conflict. The laws of armed conflict (LOAC) and the UN Charter were developed to cope with TKC, but although the fundamental principles underlying these laws remain valid, how they apply to cyber conflict in any specific instance is at best

uncertain today. The intuitions of commanders (and their legal advisors) have been honed in environments of TKC. And apart from a few specialists, an understanding of cyber conflict does not exist broadly within the personnel of today's armed forces.

CONDUCT OF CYBER CONFLICT (AND ITS CONNECTION TO KINETIC CONFLICT)

It is helpful to discuss cyber conflict in two different contexts—when overt hostilities have not broken out, and when they have broken out. These contexts are fundamentally different, because in the first as compared to the second, there is a great deal of time to prepare for the onset of conflict. That time can be used to gather intelligence and prepare the cyber "battlefield."

- Intelligence gathering. Although reliable and relevant intelligence information about an adversary has always been important in traditional kinetic conflict, it is superlatively important for cyber conflict. Because the successful penetration of an adversary's system depends on knowing its vulnerabilities and having access, intelligence is required to obtain such knowledge and access. Some such knowledge may be available from public sources; in other instances, automated means may be capable of gathering some relevant information; in still other instances, necessary knowledge may be available only through traditional spycraft. And other intelligence information is needed to develop an appropriate payload that will perform the required functions.
- Preparation of the cyber battlefield entails the identification and/or deliberate insertion of vulnerabilities into access paths to an adversary's computer systems and networks. No deliberately hostile acts are undertaken—only pre-installation of the capability to take such acts when necessary. Preparation of the cyber battlefield can be regarded as analogous to clandestinely digging a tunnel under an adversary's defensive lines. Digging a tunnel under such circumstances is a hostile action, but it is not the equivalent of initiating armed hostilities.

In the absence of intelligence information or proper battlefield preparation, cyberattacks can only be "broad-spectrum" and relatively indiscriminate or blunt. Precisely targeted cyberattacks have substantial intelligence requirements.

When overt conflict breaks out, there is less time available to collect intelligence on new cyber targets that may be identified. Thus, offensive cyber operations may have their greatest value before overt conflict breaks out or in the early stages of a conflict. (Previously identified cyber targets are vulnerable at any point in time, as long as the intelligence information remains valid and cyber-battlefield preparations remain in place. An adversary knowing that conflict is imminent or ongoing may well take measures to invalidate intelligence previously collected and/or to eliminate pre-positioned vulnerabilities or access paths.)

In addition, if TKC is involved in overt conflict, cyber operations become—in principle—just one additional tool in the arsenal of the operational commander. Assuming that legal and policy issues can be resolved (see below), cyber operations that are coordinated with kinetic operations can have powerfully synergistic effects. For example, it is common practice for operational commanders to suppress adversary air defenses to protect follow-on air strikes. Suppression can use traditional kinetic means, but cyber suppression of air defenses may be possible as well if the attacker has properly prepared the battlefield (e.g., implanted vulnerabilities in the computers controlling the air defense radars) and if adequate intelligence information is available.

SOME IMPORTANT ISSUES

Cyber conflict raises many complex issues for national security. The issues described below are intended as a sampling of the most salient, but this description is not intended to be comprehensive.

Attribution

As noted above, a key technical attribute of cyber operations is the difficulty of attributing any given cyber operation to its perpetrator. In this context, the definition of "perpetrator" can have many meanings:

- The attacking machine that is directly connected to the target. Of course, this machine—the one most proximate to the target—may well belong to an innocent third party who has no knowledge of the operation being conducted.
- The machine that launched or initiated the operation.
- The geographical location of the machine that launched or initiated the operation.
- The individual sitting at the keyboard of the initiating machine.
- The nation under whose jurisdiction the named individual falls (e.g., by virtue of his physical location when he typed the initiating commands).
- The entity under whose auspices the individual acted, if any.

In practice, a judgment of attribution is based on all available sources of information, which could include technical signatures and forensics collected regarding the act in question, intelligence information (e.g., intercepted phone calls monitoring conversations of senior leaders), prior history (e.g., similarity to previous cyber operations), and knowledge of those with incentives to conduct such operations.

It is commonly said that attribution of hostile cyber operations is impossible. The statement does have an essential kernel of truth: if the perpetrator makes no mistakes, uses techniques that have never been seen before, leaves behind no clues that point to himself, does not discuss the operation in any public or monitored forum, and does not conduct his actions

during a period in which his incentives to conduct such operations are known publicly, then identification of the perpetrator may well be impossible.

Indeed, sometimes all of these conditions are met, and policy makers rightly despair of their ability to act appropriately under such circumstances. But in other cases, the problem of attribution is not so dire, because one or more of these conditions are not met, and it may be possible to make some useful (if incomplete) judgments about attribution.

For example, even if one does not know the location of the machine that launched a given attack, signals or human intelligence might provide the identity of the entity under whose auspices the attack was launched. The latter might be all that is necessary to take further action against the perpetrator.

Deterrence and Defense in Cyberspace

A great deal of policy attention today is given to protecting information and IT that is important to the nation. There are two ways (not mutually exclusive) of providing such protection—defending one's assets against offensive actions and dissuading a hostile party from taking such actions.

Defense involves measures that decrease the likelihood that an offensive action will succeed. Such measures include those that prevent a perpetrator from a gaining access, that eliminate vulnerabilities, or that enable the victim of an operation to recover quickly from a successful offensive action.

Dissuasion involves persuading an adversary not to launch the offensive action in the first place. Deterrence is an approach to dissuasion that involves the certain imposition of high costs on an adversary that is unwise enough to initiate offensive action.

Such costs may be imposed on an identified adversary in the cyber domain in response to some hostile action in cyberspace. But there is no logical necessity for restricting a response to this domain, and decision makers have a wide choice of response options that include changes in defensive postures, law enforcement actions, economic actions, diplomacy, and military operations involving traditional forces, as well as cyber operations.

Traditionally, the U.S. national security posture has been based on a robust mix of defense and deterrence. But cyberspace turns this mix on its head. The inherent superiority of offensive cyber operations over defensive operations has led many to consider a strategy of deterrence to dissuade adversaries from conducting such operations against us. But senior policy makers have concluded that because deterrence in cyberspace is such a difficult strategy to implement, we must do a more effective job of defense.[4] If the reader finds this intellectual state of affairs unsatisfactory, s/he is not alone.

Laws of War as They Apply to Cyber Conflict

Armed conflict between nations is today governed by two bodies of international law: jus ad bellum, the body of law that governs when a nation may engage in armed conflict, and jus in bello, the body of law that regulates how

a nation engaged in armed conflict must behave. (Such law refers to treaties (written agreements among nations) and customary international law (general and consistent practices of nations followed from a sense of legal obligation).)

Today, the primary instrument of jus ad bellum is the United Nations Charter, which explicitly forbids all signatories from using force except in two instances—when authorized by the Security Council and when a signatory is exercising its inherent right of self-defense when it has been the target of an armed attack. Complications and uncertainty regarding how the UN Charter should be interpreted when cyberattacks occur result from three fundamental facts.

First, the UN Charter was written in 1945, long before the notion of cyberattacks was even imagined. The underlying experiential base for the formulation of the Charter involved TKC among nations, and thus the framers of the Charter could not have imagined how it might apply to cyber conflict.

Second, the UN Charter itself contains no definitions for certain key terms, such as "use of force," "threat of force," or "armed attack." Thus, what these terms mean cannot be understood by reference to the Charter. Definitions and meanings can only be inferred from historical precedent and practice—how individual nations, the UN itself, and international tribunals have defined these terms in particular instances. Given a lack of clarity for what these terms might mean in the context of TKC, it is not surprising that there is even less clarity for what they might mean in the context of cyber conflict.

Third, the Charter is in some ways internally inconsistent. It bans certain acts (uses of force) that could damage persons or property, but allows other acts (economic sanctions) that could damage persons or property. The use of operations not contemplated by the framers of the UN Charter—that is, cyber operations—may well magnify such inconsistencies.

An example will help to illustrate some of the complications that may arise. An offensive operation involving a number of cyberattacks conducted over time against a variety of different financial targets in an adversary nation could cause extensive economic loss, panic in the streets, and shake public confidence in the incumbent regime—but without directly causing physical damage or any loss of life. Assuming the perpetrator of this operation can be identified, on what basis, if any, would such an operation be construed under the UN Charter as a use of force or an armed attack?

Answers to such questions under various circumstances involving cyberattack matter both to the attacked party and the attacking party.

- Answers matter to **attacked** party, because they influence when and under what authority law enforcement (vis-á-vis military) takes the lead in responding, and what rights the victim might have in responding.
- Answers matter to **attacking** party, because they set a threshold that policy makers may not wish to cross in taking assertive/aggressive actions to further its interests.

Jus in bello is based in large part on the Geneva Conventions. Some of the important principles underlying *jus in bello* are the principle of non-perfidy

The International Covenant on Civil and Political Rights (ICCPR) was ratified by the United States in September 1992 and by a number of other states. Although a variety of human rights organizations strongly disagree, the United States has argued that the Convention does not apply extraterritorially, so it would not regulate the behavior of any signatory acting in any other country, whether or not it had signed the treaty.

If the contrary position is adopted, two of the rights enumerated in the ICCPR may be relevant to the cyber domain. Article 17 (protecting privacy and reputation) might be relevant to cyber operations intended to harm the reputation of an individual, e.g., by falsifying computer-based records about transactions in which he or she had engaged, or to uncover private information about an individual. Article 19 (protecting rights to seek information) might be relevant to cyberattacks intended to prevent individuals from obtaining service from the Internet or other media. A number of other rights, such as the right to life, may be implicated as well. Respecting these other rights could suggest, for example, that a cyberattack intended to enforce economic sanctions would still have to allow transactions related to the acquisition of food and medicine.

A number of nations have declared that access to the Internet is a fundamental right of their societies. (As of August 2011, these nations include Estonia, France, Spain, Finland, and Greece.) Thus, if access to the Internet is a human right, then actions curtailing or preventing Internet access violate that right.

In addition, an important and contested point in human rights law is the extent of its applicability during acknowledged armed conflict or hostilities. The position of the U.S. government is the imperatives of minimizing unnecessary human suffering are met by the requirements of the laws of armed conflict (specifically *jus in bello*), and thus that human rights law should not place additional constraints on the actions of its armed forces. By contrast, many human rights observers argue that human rights law can and should apply as well as LOAC during hostilities.

Role of Private Sector as Target and as Conductor of Offensive Cyber Operations

The private sector is deeply involved in matters related to cyber conflict in many ways—and much more so than it is involved in traditional kinetic conflict. The most obvious connection is that private sector entities are quite often the targets of hostile cyber operations. The perpetrators of most such operations against private sector entities are generally believed to be criminals (e.g., those seeking credit card numbers), but nation states may conduct cyber operations against them for a variety of purposes as well (as discussed in Section 2.3).

In addition and especially in the United States, military and civilian actors share infrastructure to a very large degree. A very large fraction of U.S. military communications pass over networks owned by the private sector and

operated largely for the benefit of civilian users. The same is true for electric power—U.S. military bases depend on the civilian power grid for day to day operations. Under many interpretations of the laws of armed conflict, military dependence on civilian infrastructure makes that civilian infrastructure a legitimate target for adversary military operations.

Another important connection is that the artifacts of cyberspace are largely developed, built, operated, and owned by private sector entities—companies that provide IT-related goods and services. In some cases, the cooperation of these entities may be needed to provide adequate defensive measures. For example, some analysts argue that an adequate defensive posture in cyberspace will require the private sector to authenticate users in such a way that anonymous behavior is no longer possible). In other cases, private sector cooperation may be needed to enable offensive cyber operations against adversaries. For example, the cooperation of a friendly Internet service provider may be needed to launch a cyberattack over the Internet.

Many questions arise regarding the private sector connection to cyber conflict. For example:

- What actions beyond changes in defense posture and calling law enforcement should private sector be allowed to take in response to hostile cyber operations? Specifically, how aggressive should private sector entities be permitted to be in their responses?
- How, and to what extent and under what circumstances, if any, should the U.S. government conduct offensive operations to respond to cyberattacks on private sector entities (or authorize an aggressive private sector response)?
- How might private sector actions interfere with U.S. government cyber operations?
- What is the U.S. government responsibility for private sector actions that rise to "use of force" (in the UN Charter sense of the term)?

Preventing Escalation and Terminating Conflict in Cyberspace

Small conflicts can sometimes grow into larger ones. Of particular concern to decision makers is the possibility that the level of violence could increase to a level not initially contemplated or desired by any party to the conflict.

In considering TKC, analysts have often thought about escalation dynamics and terminating conflict. In a cyber context, escalation dynamics refers to the possibility that initial conflict in cyberspace may grow. Much of the thinking regarding cyber conflict is focused on the first (initial) stages of conflict—what do we do if X conducts a serious cyberattack on the United States?—with the implicit assumption that such an attack is the first such cyberattack.

But what if it is not? How would escalation unfold? How could it be prevented (or deterred)? There are theories of escalation dynamics, especially in the nuclear domain, but because of the profound differences between the nuclear and cyber domains, there is every reason to expect a theory of

escalation dynamics in cyberspace would be very different from a theory of escalation dynamics in the nuclear domain. Some of the significant differences include the fact that attribution is much more uncertain, the ability of nonstate actors to interfere in the management of a conflict, and the existence of a multitude of states that have nontrivial capabilities to conduct cyber operations.

Conflict termination in cyberspace poses many difficulties as well. Conflict termination is the task faced by decision makers on both sides when they have agreed to cease hostilities. A key issue in implementing such agreements is knowing that the other side is abiding by the negotiated terms. How would one side know that the other side is honoring a cease-fire in cyberspace, given that one or both sides are likely to be targets of hostile cyber operations from other parties that do not cease just because there is cyber conflict between the two principal actors? (That is, there is a constant background of hostile cyber-operations going on all the time.) And might one side have to inform the other of all of the battlefield preparations it had undertaken prior to the conflict? Such an act, analogous to demining operations, would require each side to keep careful track of its various preparations.

Escalation can occur through a number of mechanisms (which may or may not simultaneously be operative in any instance).[5] One party to a conflict may deliberately escalate a conflict, with a specific purpose in mind. It might inadvertently escalate a conflict by taking an action that it does not believe is escalatory but that its opponent perceives as escalatory. It might accidentally escalate a conflict if its forces take some unintended action (e.g., they strike the wrong target). Lastly, catalytic escalation occurs when some third party succeeds in provoking two parties to engage in conflict ("let's you and him fight"). Catalytic provocation is facilitated by the possibility of anonymous or unattributable action.

CONCLUSION

Conflict can and does occur in cyberspace. How and to what extent does recent history about conflict in cyberspace presage the future?

Two things are clear today. First, only a small fraction of the possibilities for cyber conflict have been experienced to date, and actual experience with cyber conflict has been limited. Indeed, nearly all of the adversarial actions known to have been taken in cyberspace against the United States or any other nation, including both cyberattack and cyberexploitation, have fallen short of any plausible threshold for defining "armed conflict," "use of force," or "armed attack." This fact has two consequences: many possibilities for serious cyber conflict have not yet been seen,[6] and how to respond to hostile actions in cyberspace that do not rise to these thresholds is the most pressing concern of policy makers today.

Second, many of our assumptions and understandings about conflict—developed in the context of traditional kinetic conflict—either are not valid in cyberspace or are applicable only with difficulty. Thus, decision makers are proceeding into largely unknown territory—a fact that decreases the predictability of the outcome of any actions they might take.

These conclusions suggest that the need to develop new knowledge and insight into technical and legal instruments to support informed policy making in this area will provide full employment for many analysts for a long time to come.

NOTES

1. The intellectual content of this report is drawn primarily from National Research Council, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (William Owens, Kenneth Dam, Herbert Lin, editors), National Academies Press, 2009, available at http://www.nap.edu/catalog.php?record_id=12651.
2. This definition implies that "armed conflict" or "military conflict" are subsets—and only subsets—of the broader term "conflict," which may entail a conflict over economic, cultural, diplomatic, and other interests as well as conflict involving military matters or the use of arms.
3. A primer on Stuxnet can be found at http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html?scp=1-spot&sq=stuxnet&st=cse.
4. William Lynn, "Defending a New Domain: the Pentagon's Cyberstrategy," *Foreign Affairs,* September/October 2010.
5. RAND, *Dangerous Thresholds: Managing Escalation in the 21st Century,* 2008, available at www.rand.org/pubs/monographs/2008/RAND_MG614.pdf.
6. Gregory Rattray and Jason Healey, "Categorizing and Understanding Offensive Cyber Capabilities and Their Use," in National Research Council, *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy,* National Academies Press, 2010, pp. 77–98, available at http://www.nap.edu/catalog/12997.html.

After Egypt: The Limits and Promise of Online Challenges to the Authoritarian Arab State

MARC LYNCH

On December 17, 2010, the self-immolation of a young man in a Tunisian village set off a chain of events which culminated in massive protests across the country and the fall of the long-ruling dictator Zine el-Abidine Ben Ali. The riveting spectacle of these protests on al-Jazeera, widely discussed across both the online and offline Arab public sphere, soon sparked imitators across the region. The protests largely bypassed formal political parties and

From Marc Lynch,"After Egypt: The Limits and Promise of Online Challenges to the Authoritarian Arab State" in *Perspectives on Politics,* Vol. 9, Issue 2. Portions of the text and all footnotes have been omitted.

International Politics

Enduring Concepts and Contemporary Issues

Eleventh Edition

ROBERT J. ART

Brandeis University

ROBERT JERVIS

Columbia University

PEARSON

Boston Columbus Indianapolis New York San Francisco Upper Saddle River
Amsterdam Cape Town Dubai London Madrid Milan Munich Paris Montreal Toronto
Delhi Mexico City São Paulo Sydney Hong Kong Seoul Singapore Taipei Tokyo

Senior Acquisitions Editor: Vikram Mukhija
Editorial Assistants: Isabel Schwab, Beverly Fong
Executive Marketing Manager: Wendy Gordon
Production Manager: Denise J. Phillip
Project Coordination, Text Design, and
Electronic Page Makeup: Laserwords Pvt Ltd, India
Cover Design Manager: John Callahan
Cover Designer: Kay Petronio
Cover Image: Veer, Inc.
Senior Manufacturing Buyer: Roy Pickering
Printer/Binder: R.R. Donnelley/Crawfordsville
Cover Printer: R.R. Donnelley/Crawfordsville

Credits and acknowledgments borrowed from other sources and reproduced, with permission, in this textbook appear on the appropriate page within the text.

Library of Congress Cataloging-in-Publication Data
International politics : enduring concepts and contemporary issues / [edited] by Robert J. Art, Robert Jervis.—11th ed.
p. cm.
ISBN 0-205-85164-9 (alk. paper)
1. International relations. 2. World politics—1989- 3. Globalization.
I. Art, Robert J. II. Jervis, Robert, 1940-
JZ1242.I574 2012
327—dc23
2011052931

10 9 8 7 6 5 4 3 2 1—DOC—15 14 13 12

PEARSON

ISBN 10: 0-205-85164-9
ISBN 13: 978-0-205-85164-5