Ethics and Information Technology (2005) 7:61–73
DOI 10.1007/s10676-005-4582-3


# Where computer security meets national security[1]

Helen Nissenbaum
*Department of Culture and Communication, New York University, NY, USA*
*E-mail: helen.nissenbaum@nyu.edu*

**Abstract.** This paper identifies two conceptions of security in contemporary concerns over the vulnerability of computers and networks to hostile attack. One is derived from individual-focused conceptions of computer security developed in computer science and engineering. The other is informed by the concerns of national security agencies of government as well as those of corporate intellectual property owners. A comparative evaluation of these two conceptions utilizes the theoretical construct of "securitization," developed by the Copenhagen School of International Relations.

**Key words:** cyber-security, computer security, securitization

## Introduction

Over the course of the past decade, the mandate of computer security has grown in complexity and seriousness as information technologies have saturated society and, simultaneously, the threats have multiplied in number and sophistication. Although widely publicized attacks such as denial-of-service, viruses, worms and unauthorized break-ins create the impression that the work of computer security specialists is clear-cut, this paper holds that the broad purpose of computer security, in fact, is ambiguous. At least two prominent conceptions of security vie for the attention and resources of experts, policy makers, and public opinion. One, focusing on individual systems and networks, has its roots in computer science and engineering communities. The other, a more recent entry, focuses on collective and institutional systems, reflecting the influence of political and national security actors. Currently, these two conceptions exist side-by-side. But their inherent differences spell tensions in future social, political, and technical decision-making.

The purpose of this paper is to elaborate the sources and implications of these tensions so as to help guide choices. Although a full account would address outcomes in social, political, and technical arenas, this paper focuses mainly on the technical, asking, for this arena, how the two conceptions of security are likely to play out and what reasons we might have for favoring one conception over the other. The decision to focus on implications for technical choices is not arbitrary but comes from one of the key motivating interests of this paper, namely, how values, generally, are embodied in technical systems and devices (henceforth "technologies"), both in their design and regulation. Before picking up the paper's main thread, we take a brief detour on the subject of values in design of technologies showing how it has shaped our questions about security.

## Values in technical design

A significant body of work in the humanistic and social study of technology advances an understanding of technology not merely as an independent material form which acts on people and societies but as

[1] This article has been on the drawing boards for longer than I dare to admit. Along the way, many have helped its development by generously sharing their wisdom: James Der Derian, Niva Elkin-Koren, Ed Felten, Batya Friedman, Lene Hansen, audiences at CEPE, TPRC, the Yale Cybercrime and Digital Law Enforcement Conference, and Watson Institute's Symposium in Dis/Simulations of War and Peace," and University of Newcastle, Computer Science Department. Thanks, also, to Sam Howard-Spink for excellent editorial assistance.

political to its very core. That technical systems and devices can serve as venues for political struggle has found expression in a range of scholarly works, from Langdon Winner's famous assertion that artifacts "have politics" (1986)[2] to lesser known claims such as Bryan Pfaffenberger's that STS (Science and Technology Studies) be conceived as "the political philosophy of our time."[3] While a large and excellent body of scholarship in STS and philosophy of technology has produced theories and case analyses that convincingly argue in favor of this fundamental claim, recent initiatives, spearheaded in the context of computer and information technologies, focus on the practical question of how to bring these ideas to bear on the design of the information and communications systems that increasingly shape the opportunities and daily experiences of people living in technologically advanced societies. The rationale behind this pragmatic turn is this: if values shape technical systems, then responsible creators and regulators should trust neither serendipity nor possibly illegitimate agency to produce the best outcomes. Ethical and political values ought to be added to traditional considerations and constraints guiding the design and regulation of these systems, such as functionality, efficiency, elegance, safety, and, more recently, usability.

Although we are still at the early stages of formulating appropriate methodological principles, this much is clear: implementing values in the design and regulation of information and communications technologies requires not only technical (engineering and scientific) adeptness and a firm empirical grounding in how people perceive and are affected by them (as may be learned from usability studies, surveys, etc.), but also an adequate grasp of key conceptual definitions as well normative theories in which these are embedded. It is laudable for well-meaning designers and developers to seek (Friedman, Kahn Jr. and Borning (forthcoming), Camp (2003), Camp and Osorio (2002), Flanagan, Howe and Nissenbaum (forthcoming), Nissenbaum (2004, forthcoming); Benkler and Nissenbaum (forthcoming[4]) for example, to preserve privacy, or provide accessibility to the disabled, of promote sociality and cooperation. However, unless such interventions are guided by sound concepts of privacy, equity, welfare, and cooperation, respectively, and well-reasoned, theoretically grounded justifications for choices and trade-offs, their efforts could easily miss the mark. For this reason, it is of far more than "academic" interest to ponder the meaning of "security" in computer security given that which of the two (or possibly other) meanings of security guides the choices of designers and regulators could have a significant effect on outcomes for the users of computers and networked information systems. This paper aims to sketch some of the alternatives that are likely to follow our two interpretations of security.

Security deserves a place alongside privacy, intellectual property, equity, and other values that have been vigorously debated in light of developments in and application of digital electronic information technologies. So far, security has been treated primarily as a technical problem, despite its being a rich, complex, and contested concept with variable shadings of specialized and general meanings. Like the values mentioned above security, too, has been stretched and challenged by radical alterations in information and communications environments generated by computing and networks. It is important to understand what precisely it is that is being sought and sometimes achieved in the technologies

[2] L. Winner. *Do Artifacts have Politics? The Whale and the Reactor: A Search for Limits in an Age of High Technology*. University of Chicago Press, Chicago, 1986.

[3] B. Pfaffenberger. "Technological Dramas." *Science, Technology & Human*, 17(3): 282–312, 1992.

[4] See at the project "Value in Technology Design: Democracy, Autonomy, and Justice," available at: [http://www.nyu.edu/projects/valuesindesign/]; B. Friedman, P.H. Kahn, Jr. and A. Borning, "A Value Sensitive Design and Information Systems", forthcoming. In P. Zhang and D. Galletta, editors, *Human-Computer Interaction in Management Information Systems: Foundations*. M.E. Sharpe, Inc, NY; Camp I. Jean, "Design for Trust". In Rino Falcone, editor, *Trust, Reputation and Security: Theories and Practice*: Aamas 2002 International Workshop, Bologna, Italy, July 15, 2002: Selected and Invited Papers (Lecture Notes in Artificial Intelligence). Springer-Verlag, Berlin, 2003; L. Jean Camp & Carlos Osorio, "Privacy Enhancing Technologies for Internet Commerce". In *Trust in the Network Economy*. Springer-Verlag, Berlin, 2002; Flanagan, Howe and Nissenbaum (forthcoming); H. Nissenbaum. "Will Security Enhance Trust Online, or Supplant It?" In M.R. Kramer and S.K. Cook, editors, *Trust and Distrust in Organizations: Dilemmas and Approaches Volume VII* in the Russell Sage Foundation Series on Trust. Russell Sage Foundation, New York, 2004; Benkler Y. and Nissenbaum H. (forthcoming), "Commons Based Peer Production and Virtue."

and regulations aspiring to produce a state of security. If we can unambiguously describe the valued outcome that is the goal of computer (and network) security, then, at the very least, we will be better qualified to judge whether the vast and loosely connected community of scientists and engineers working in academia, governmental and corporate research institutions, and in backrooms of enumerable private and public organizations and businesses is achieving its mission. Finally, an explicit expression of the goal, or goals, of security efforts will make an evaluation of these goals possible: are the goals morally grounded, are they worth pursuing, and, if so, at what cost?

## Two conceptions of computer security

Taking note of what has been said, over the past few years, about the mission of computer security, two conceptions seem dominant. One, here labeled "technical computer security," has roots in the scientific and technical field of the same name and has been developed and articulated by the field's leaders in such venues as professional conferences, scholarly and research journals, and committee reports of the National Research Council.[5] The other, here labeled "cyber-security," a more recent entry to the public sphere, is typically articulated by government authorities, corporate heads, and leaders of other non-governmental sectors. It links computer security to traditional notions of national security. At present, these two conceptions exist side-by-side, each one angling for the attention of key social actors including government agencies, technical experts and institutions, corporations, policy experts, pundits, the general public, and, importantly, the media (popular as well as specialized.)

The two conceptions, while not strictly incompatible on all points, emphasize different issues and, as a result, pull in different directions. In order to understand why these differences are significant, we need to flesh them out a little more.

## Technical computer security

Within the technical community, the traditional core mission of computer (and network) security has been defined by three goals: availability; integrity; and confidentiality. In other words, the work of technical experts in the field of computer security has generally focused on protecting computer systems and their users against attacks, and threats of attack, in three general categories:

- Attacks that render systems, information, and networks unavailable to users, including for example, denial-of-service attacks and malware such as viruses, worms, etc. that disable systems or parts of them.
- Attacks that threaten the integrity of information or of systems and networks by corrupting data, destroying files or disrupting code, etc.
- Attacks that threaten the confidentiality of information and communications, such as interception of emails, unauthorized access to systems and data, spyware that enables third parties to learn about system configuration or web browsing habits.

Although instantiations of these types of attacks have evolved over time, the categories have remained surprisingly robust. This is not to say that the field has remained static as each new form of even the same type of attack requires novel defenses. Those who undertake to provide security understand that their actions may not lead to total and permanent invulnerability, but at best a temporary advantage against wily adversaries who themselves are engaged in a race in continually evolving tools for penetrating these defenses. Further, the boundaries of what is included in technical security continues to expand to meet new applications. For example, as electronic commerce has become more common, security experts have sought technical means to authenticate identities and prevent repudiation of financial commitment. Some have argued for extending the mission of technical security even further to the broader concept of "trustworthiness," which includes features such as survivability and dependability not only in the face of deliberate attack but also accidental failures. (See for example the CSTB report on Trust in Cyberspace and DIRC project definition.)[6] For

[5] National Research Council, *The Internet Under Crisis Conditions*, (The National Academies Press, Washington, D.C., 2003); Hennessy L. J, Patterson A. D. and Lin S. H. (eds.) (2003), *Information Technology for Counterterrorism*, (The National Academies Press, Washingtom D.C., 2003); Baskerville R. (1993), "Information Systems Design Methods: Implications for Information Systems Development," 25(4) *ACM Computing Surveys*, pp. 375–414.

[6] "Trust in Cyberspace," Committee on Information Systems Trustworthiness, National Research Council (1999) available at: [http://www.nap.edu/readingroom/books/trust/]; see the society's dependability definition by the DIRC project, available at: [http://www.dirc.org.uk/overview/index.html].

purposes of the discussion here, we will assume the narrower conception of computer security focusing on protection against deliberate attack.

## Cyber-security

In the conception that I will call cyber-security, the issues of greatest danger fall roughly into three categories:

1. Threats posed by the use of networked computers as a medium or staging ground for antisocial, disruptive, or dangerous organizations and communications. These include, for example, the websites of various racial and ethnic hate groups, sites that coordinate the planning and perpetration of crimes (especially fraud), websites and other mechanisms that deliver child-pornography, and – perhaps of most urgent concern as of the writing of this paper – use of the Internet for inducing terrorist actions and for the operational planning of terrorist attacks (Bendrath 2003).[7]
2. Threats of attack on critical societal infrastructures, including utilities, banking, government administration, education, healthcare, manufacturing and communications media. Here, the argument is that because critical systems are increasingly dependent on networked information systems, they are vulnerable to network attacks. Potential attackers include rogue U.S. nationals, international terrorist organizations, or hostile nations engaging in "cyber-war."
3. Threats to the networked information system itself ranging from disablement of various kinds and degrees to – in the worst case – complete debility.[8]

The central claim of this article is that two conceptions of security seem to drive efforts in computer (and network) security and that their differences are significant for regulation and design. A difference that is most immediately obvious is scope: cyber-security overlaps with technical security but encompasses more. Scope, as I argue below, is not all that separates the two. Other differences will become evident as we develop the two conceptions through a series of questions, beginning with the most rudimentary: why security? In other words, why are the issues raised by the two conceptions matters of security? Closely connected with this is a second, basic question: what contributes to the moral force of computer security, so conceived?

## Security and its moral force

A foundational assumption of both conceptions is that the material concerns they raise are rightly construed as security concerns. Although this apparently self-evident proposition may prove unproblematic, it is worth taking a moment to draw the connection explicitly, starting with a general or ordinary account of security as safety, freedom from the unwanted effects of another's actions (Ripstein 1999),[9] the condition of being protected from danger, injury, attack (physical and non-physical), and other harms, and protection against threats of all kinds. From here, the question to ask is why the activities cited by various accounts of computer security warrant the label of "threat of harm," against which people deserve to be secured.

With technical computer security, the promise is protection against attacks by adversaries whose actions deprive victims of access to or use of systems and networks (availability); damaging, spoiling, or altering their systems or data (integrity); and revealing or diverting information to inappropriate recipients (confidentiality). These are security concerns to the extent we agree that the attacks in question, in the context of computing, information flow, digital electronic communication, etc., constitute harm. This is key and not as obvious as it might at first appear. It is important because the quest for computer security has moral force only to the extent that it promotes the common value of freedom from harm. In other words, the issue is not merely why these are classifiable as security concerns but why people *deserve*, or have a right, to be thus secured.

---

[7] Bendrath, R. "The American Cyber-Angst and the Real World–Any Link?" In R. Latham, editor, *Bombs and Bandwidth*, pp. 49–73. The New Press, New York, 2003.

[8] According to the "The National Strategy to Secure Cyberspace," Feb. 2003 (available at: http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf) cyber-attacks on U.S. information networks can have serious consequences such as disrupting critical operations, loss of revenue and intellectual property, or loss of life; see also United State Senate, Committee on the Judiciary, Testimony of Mr. Keith Lourdeau, FBI Deputy Assistant Director, Cyber Division, February 24, 2004 (available at: http://judiciary.senate.gov/testimony.cfm?id=1054&wit_id = 2995).

[9] R. Arthur. "Prohibition and Preemption," In *5 Legal Theory*, pp. 235–263, Cambridge University Press, 1999.

Antithetical to this picture is a more cynical view of the goals of technical computer security as a quest for increasingly effective ways to protect individuals and institutions against actions that threaten the fulfillment of desires and subjective preferences, irrespective of their moral standing. Ross Anderson (2003), a computer scientist who also comments on policy implications of the technology, presents such a turn in computer security – driven more by what customers want than by a mission to provide protection against objectively (or inter-subjectively) construed harm. Illustrative cases are moves by corporate entities to secure their assets and market standing including, for example, Microsoft, creating so-called "trusted computing" which would restrict individuals in the way they use their computers, particularly in relation to proprietary information. Anderson cites Hewlett-Packard as another example, applying cryptographic techniques to prevent consumers from installing third-party printer cartridges in HP printers. Cases like these portray computer security as an amoral practice and security engineers as guns for hire working to promote vested interests (securing parochial benefits) rather than as agents of public good.[10]

If technical computer security were directed *only* to the task of securing the private interests of stakeholders who could afford such protection, it could not sustain the compelling claim on *public* attention, approbation, and financial investment that it currently holds. Our point of departure, therefore, is that the focus is broader in two ways. First, the implicit beneficiaries of computer security are everyone who uses, owns, or possibly even is affected by computers and networks, including ordinary persons as well as individual institutional agents of any size. Second, still to be shown, is that the promised benefits are generally valued by the relevant surrounding communities. By implication, computer security is a value, and the activities of technical security experts are of moral import, if the stated end toward which they are directed result in protection from (conditions generally thought to be) harms.

More specifically, it is not surprising that a society that values the institution of private property and understands computer systems and information as possible forms of property would value integrity given that assaults on system integrity can easily be construed as a form of property damage. Further, since confidentiality is typically a valued aspect of privacy, intrusions into systems or communications are readily conceived as instances of harm. The case of system and data availability is slightly more complex as one could argue for its protection on grounds of traditional property rights (both "use and enjoyment") and the owner's entitlement to alienate the property in question from others. But denying a user availability also constitutes a violation of autonomy as it interferes with an increasingly important means of identity formation as well as pursuit of self-determined ends. Because system availability, integrity, and confidentiality are also instrumental to achieving other ends, such as safe commercial transactions, productivity, robust communication, and more, threats to them may be harmful in many ways beyond those listed above.

When the two foundational questions are asked of cyber-security, namely, why are the issues it raises matters of security and what are the sources of its moral weight, the answers are different. I argue that, here, the meaning of security is drawn not from ordinary usage but from usage developed in the specialized arena of national security. The difference, therefore, is not merely one of scope but of meaning, and what follows from this difference is of practical significance. The argument is inspired by insights and a vocabulary developed within the Copenhagen School of thought in the area of international security studies.

## Securitization: The Copenhagen School[11]

In the field of international security studies, traditional approaches frequently called "realist" have been challenged by those taking more general and "discursive" ones. As depicted by these challengers, realist theories adopt an overly narrow view of national security, focusing on protection of physical borders and strategic assets against military attacks by foreign states. The broader view includes not only terrorist attacks occurring within national borders but threats other than military ones. Also resisting the realists' treatment of threats as objectively conceived and characterized, some of the challengers opt for so-called constructivist or discursive accounts of national and international security. One such approach, offered by

[10] R. Anderson. "Cryptography and Competition Policy–Issues with Issues with Trusted Computing." In *Proceedings Workshop on Economics and Information Sector*, pp. 1–11, 2003.

[11] For a description of this approach to security studies, I have used B. Buzan, O. Wyer, J.D. Wilde and O. Waever, *Security: A New Framework for Analysis*, Lynne Rienner Publishers, Inc., Boulder, 1997; O. Waever, "Concepts of Security," Ph.D. dissertation. Institute of Political Science, University of Copenhagen, 1995.

the Copenhagen School, whose key proponents are Barry Buzan and Ole Waever, provides a useful framework for articulating differences between conceptions of security in Cyber-security and technical computer security. Any further discussion of differences between realist and discursive approaches to security studies, however, lie beyond the scope of this paper.

In proposing a constructivist framework, Buzan and Waever are less concerned with providing an objective characterization of threats, vulnerabilities, and modes of defense, and more with providing a systematic account of the ways specific conditions, states-of-affairs, or events are posed by significant social actors as threats to security and come to be widely accepted as such. They call this rendering of a security threat "securitization," which becomes the fundamental explanatory construct of their framework. Before using the notion of securitization to highlight differences between the two conceptions of security in computer security, a few more features of the framework need to be specified.

The concept of securitization generalizes certain elements of traditional approaches to national security in which the typical landscape includes a threat of military attack, the nation-state under threat, and the specific steps leaders take to ensure the state's continued security (through such means as defensive action, shoring up vulnerabilities, and so forth.) The Copenhagen School moves from this landscape to one in which the threat need not be military and the referent object need not be the state. Further, its assertions are not about actual threats, referent objects, and defensive maneuvers, but about the successful portrayal of threats as security threats and what this means. Accordingly, the questions that concern Buzan, Waever, and their colleagues are about the typical threats, agents, and referent objects that characterize conditions in which securitization of a threat is attempted and also in which securitization of that threat succeeds. We briefly summarize some of their answers.

From the traditional conception of security in national security, this account moves away from the paradigmatic military threat to a more general notion. What it retains as a key feature of threats capable of being securitized is that they be presented not merely as harmful but as dire, imminent and existential. A threat must be presented to an audience and accepted by that audience as fatal to a referent object's very existence. These are life-and-death threats, existential threats to a group, a valued entity, a way of life, or ideology. In the case of the state, a securitized harm is one that threatens national sovereignty and political autonomy, of subjugation by a foreign will. Presenting something as a threat to a society, culture, or religion, involves claiming it as a critical challenge to social, religious, or cultural identity, to an historical way of life, to hallowed traditions.

A similar extension occurs in what can count as the referent object – not only the state but other entities as well. The field is not entirely open. Buzan and Waever argue that only general collectives or collective values count as such. Only entities that an audience believes *have* to survive are likely to rouse the necessary degree of salience and concern. The nation-state, at least in the present era, is an obvious contender but so are such valued entities as environment, religion, culture, economy, and so on. Obviously the range of threats will vary in relation to entities, thus pollution may be a dire threat for the environment, depression a dire threat to an economy, assimilation for a religion and so on. Referent objects highly unlikely to be securitized include specific individuals, or what Buzan and Waever call mid-level, limited collectives like firms, institutions, or clubs, even if threats in question are existential. Exception might occur if a clear link can be drawn between the survival of the mid-level entity and the greater collective.[12] The threat of Japanese automakers, for example, to the profitability of the Ford automobile company, or even to its continued existence, is unlikely to be securitized unless proponents are able to launch a convincing argument that Ford's demise will lead to a crash in the entire economy.

In general, to securitize an activity or state-of-affairs is to present it as an urgent, imminent, extensive, and existential threat to a significant collective.

A third important aspect of the framework is agency. One half of the story is who has the capacity or power to securitize, to be a securitizing actor. These typically will include high-ranking government officials – elected or appointed, members of cabinet, high-ranking military personnel, the president (or prime minister.) It is possible, however, that others in a society might have achieved sufficient salience and persuasive capacity to construct the conception of threat necessary for securitization. One could imagine that trusted media sources, high ranking jurists, and possibly corporate personalities might accumulate this degree of salience. It is also possible that highly visible lobbyists, pressure groups, and the public media might have the capacity indirectly to move government officials toward securitizing given threats. The other half of the story is whether securitizing moves are accepted. Here, we must settle for

[12] B. Buzan, O. Wyer, J.D. Wilde and O. Waever, *Security: A New Framework for Analysis*, p. 32. Lynne Rienner Publishers, Inc., Boulder, 1997.

something like a preponderance of views in the larger social or national context. Most importantly, however, in order for securitization of a threat to have succeeded we need both securitizing moves by relevant actors as well as acceptance by the surrounding communities.

## Application to cyber-security

Examining in greater detail ways in which the three categories of threats to cyber-security have been presented by prominent voices in government, the private sector, and media, we can detect clear moves to securitize. These moves invest cyber-security with the specialized meanings of securitization, in contrast with what I above called the general or ordinary meaning. In these moves, the dangers in question are posed as imminent, urgent, and dire for the United States and the rest of the free world.

The first threat category stems from the far-reaching power of the "new medium" to serve as a highly effective tool for one-to-one and many-to-many interactive communication, as well as one-to-many broadcast communication. Even prior to the attacks of 11th September, 2001, the media played up government worries over the dangerous potential of the net. In February 2001, for example, *USA Today* published a widely cited article claiming that government officials feared Al Queda was using steganography, a cryptographic method for concealing secret information within another message or digital image, to convey instructions for terrorist attacks and for posting blueprints of targets on websites, such as sports chat rooms and pornographic bulletin boards.[13] Ralf Bendrath cites Leslie G. Wiser, Jr.'s testimony before the House of Representatives in August 2001, asserting that terrorist groups are using the Internet to "formulate plans, raise funds, spread propaganda, and to communicate securely."[14]

In the period following the attacks, these themes crop up regularly in the public media, as, for example, in this news report:

> Today bin Laden is believed to school his soldiers in high-tech tools of communication. E-mail, online dead drops, satellite phones, cell phones, encryption and digital camouflage called steganography ... are all tools of Al Qaeda, bin Laden's terrorist network. Those high-tech tools enable members of Al Qaeda to communicate with terrorist cells (or groups) hidden around the world.[15]

Another article reports about Al Qaeda communication strategy as described by one of its members, captured by the U.S.:

> The Qaeda communications system that Mr. Khan used and helped operate relied on websites and e-mail addresses in Turkey, Nigeria and the northwestern tribal areas of Pakistan, according to the information provided by a Pakistani intelligence official.
>
> The official said Mr. Khan had told investigators that couriers carried handwritten messages or computer disks from senior Qaeda leaders hiding in isolated border areas to hard-line religious schools in Pakistan's Northwest Frontier Province.
>
> Other couriers then ferried them to Mr. Khan on the other side of the country in the eastern city of Lahore, and the computer expert then posted the messages in code on Web sites or relayed them electronically, the Pakistani official said.
>
> Mr. Khan had told investigators that most of Al Qaeda's communications were now done through the Internet, the official said.[16]

The second and third threat categories, presented as catastrophic cyber-attacks and debilitating assaults on critical infrastructure have been aired in dramatic terms. In the following lengthy quotation from a January 7, 2000, White House press briefing, moves to securitize are evident as Chief of Staff John Podesta, Secretary of Commerce Bill Daley, James Madison University President Linwood Rose, and National Coordinator for Security, Infrastructure Protection and Counter-Terrorism Dick Clarke, answer questions about computer and network security.

---

[13] J. Kelley, "Terror Groups Hide Behind Web Encryption," *USA Today* (February 6, 2001) discussed in McCullagh D. (2001), "bin Laden: Steganography Master?" *Wired News* (February 7, 2001), available at: [http://www.wired.com/news/print/0,1294,41658,00.html].

[14] R. Bendrath, "The American Cyber-Angst and the Real World – Any Link?" In *Bombs and Bandwidth* (2003) Robert Latham (ed.) (New York: The New Press), pp. 49–73.

[15] Gaudin, S. "The Terrorist Network," *NetworkWorldFusion* (November 26, 2001). Available at: [http://www.nwfusion.com/research/2001/1126featside4.html].

[16] D. Jehl and D. Rohde, "Captured Qaeda Figure Led Way To Information Behind Warning," *The New York Times*, 2004.

JOHN PODESTA: "And just as in the 1950s when we were building an economy based on a new transportation system, a new interstate highway system and we put guardrails on that transportation system, we're here today to talk about how we can better protect the information technology and infrastructure of the information technology economy – not only for the government, but for the private sector, as well....
"... It's not just computers; it's the electric power grid, it's the other things that we learned so much about during our run-up to Y2K. The banking, financial industry – increasingly every single sector of the economy is tied in, linked through e-commerce, through the use of computer technology, to this kind of critical infrastructure that has developed over the course of the 1970s, 1980s and 1990s."

SECRETARY DALEY: " ... no question, we have a new economy and we have an economy that is much more dependent, as we enter this next century, on information technologies. So our defending of this economy is most important to us... One of the consequences of leading this e-world is that we, as I mentioned, are more dependent on information technologies in our country, and therefore we're more subject to new and different kinds of threats."
Q: "What's the biggest threat that you're trying to guard against? Is it hackers and vandalism? Is it criminals? Or is it domestic or foreign terrorism?"
MR. CLARKE: "I think it's all of the above. There's a spectrum, from the teenage hacker who sort of joy rides through cyberspace, up through industrial espionage, up through fraud and theft. And up at the far end of the spectrum, to another country using information warfare against our infrastructure."
SECRETARY DALEY: "This is the first time in American history that we in the federal government, alone, cannot protect our infrastructure. We can't hire an army or a police force that's large enough to protect all of America's cell phones or pagers or computer networks – not when 95 percent of these infrastructures are owned and operated by the private sector."

Picking up on themes of critical dependencies on information networks, endorsement for moves to securitize comes not only from government authorities or other representatives of public interests but from corporate owners of intellectual property. They have tried, with some success, to hitch their star to the security wagon by claiming not only that rampant unauthorized copying and distribution of proprietary works poses an existential threat to their business but by presenting their possible demise as a dire threat to the U.S. economy. They have singled out as the "dangerous" activity from which we ought to be protected: out-of-control peer-to-peer (p2p) file sharing.[17]

The Net itself has been posed as a potential battlefield for comprehensive attack on the state.[18] According to this picture, warfare waged online through computer viruses, worms, and other malware could serve an enemy's strategic ends by disrupting "access or flow of forces" to a sensitive region.[19] A similar notion is embodied in remarks made by Secretary of Defense Donald Rumsfeld, at a June 6, 2001, meeting of the NATO Council, where he referred to the dangers of "attacks from cyberspace." This rather murky reference, nevertheless, conveys a sense of cyberspace as potentially an embattled frontier.[20] Imparting a sense of the magnitude and seriousness of cyber-threats, Curt Weldon, chairman of the National Security Committee's subcommittee on military research and development invokes a powerful national memory: "It's not a matter of if America has an electronic Pearl Harbor, it's a matter of when."[21]

For those who warn of cyberspace as a staging ground for aggressive attack on the nation, another reason not to underestimate the dangers inherent in the networked information infrastructure is asymmetry. The Net enables a magnitude of damage

[17] For example, the testimony of Jack Valenti, President and CEO Motion Picture Association of America, before the SubCommittee on Courts, the Internet, and Intellectual Property Committee on the Judiciary U.S. House of Representatives, "International Copyright Piracy: Links to Organized Crime and Terrorism" (March 13, 2003) available at: [http://www.house.gov/judiciary/valenti031303.htm].

[18] An official rendering of threats and vulnerabilities in the context of national security concerns can be seen in *The National Strategy to Secure Cyberspace*, February 2003, a report by President George W. Bush's Critical Infrastructure Protection Board (headed by Richard A. Clarke), especially the chapter, "Cyberspace Threats and Vulnerabilities: A Case for Action."

[19] R. Bendrath. "The American Cyber-Angst and the Real World–Any Link?" In R. Latham, editor, *Bombs and Bandwidth*, p.56. New York, The New Press, 2003, quoting Admiral Thomas R. Wilson's comments during a hearing of Senate Select Committee on Intelligence, February 2001.

[20] R. Bendrath. "The American Cyber-Angst and the Real World–Any Link?" In R. Latham, editor, *Bombs and Bandwidth*, p. 57. The New Press, New York, 2003.

[21] K. Mitnick. "Hacker in Shackles," The Guardian (London), 1999.

hugely disproportional to the size and relative strength – measured in conventional terms – of an attacker. Experience has shown that even a single, not especially skilled attacker can cause considerable inconvenience, if not outright damage. This means that the U.S. must guard against the usual array of world powers, as well as all adversaries with sufficient technical know-how. In official statements about cyber-security adversaries of many types are mentioned, from malevolent teenagers, common or organized criminals and terrorists, to hostile nations. According to Bendrath, successive U.S. administrations under Bill Clinton and George W. Bush have cycled through opinions over the source of greatest concern, whether organized criminals, terrorists, or hostile states. For a country like the U.S., which is in a position to draw confidence from its size and strength, the notion of a small but disproportionately destructive "asymmetric threat," challenges national security orthodoxy and deepens collective worry.

## Contrasts

The point of the discussion so far has been to educe contrasts in the conceptions of security informing technical computer security and cyber-security, respectively. Above, I claimed that the contrast went beyond that of scope. One is to be found in the degree of severity and nature of the threats. The former acknowledges a broader variation in both degree of harm and the type of harm, including damage to property, incursions on autonomy, privacy, and productivity. The latter, in securitizing threats, assumes the threats to be dire, and possibly existential. A second contrast is in the prototypical referent object. The former seeks security primarily for individual nodes (people, agents, institutions) the latter focuses on collective security (state or nation). A third contrast can be found in the sources of moral force, that is in the justifications each offers for actions taken in the name of security.

## The practical importance of securitization

Asked another way, the question about moral force is about why we should care that two conceptions of security inform computer security – why the difference matters. The answer, beyond mere enlightenment, lies in the defensive activities that each of the conceptions warrants. More will be said below about the range of responses to threats recommended by proponents of technical computer security – similar in nature to reactions one would expect to unethical, including criminal, actions. By contrast, the logic of national security, which informs those who move to securitize online threats, calls for extraordinary responses; security discourse not only heightens the salience and priority of designated threats but bestows legitimacy on a particular range of reactions.[22] As observed by James Der Derian:

> No other concept in international relations packs the metaphysical punch, nor commands the disciplinary power of 'security.' In its name peoples have alienated their fears, rights and powers to gods, emperors, and most recently, sovereign states, all to protect themselves from the vicissitudes of nature – as well as from other gods, emperors, and sovereign states. In its name weapons of mass destruction have been developed which transfigured national interest into a security dilemma based on a suicide pact. And, less often noted in IR, in its name billions have been made and millions killed while scientific knowledge has been furthered and intellectual dissent muted.[23]

Similarly Buzan, Waever and de Wilde write, "What is essential (to securitization) is the designation of an existential threat requiring emergency action or special measures and the acceptance of that designation by a significant audience."[24] These "special measures" typically involve bending rules of normal governance, and as matters of national security they are lifted – presumably temporarily – outside, or beyond the bounds of political procedure.[25] In the face of securitized threats and times of national crises, even liberal democracies accept breaks from "busi-

[22] H. Lene. "The Little Mermaid's Silent Security Dilemma and the Absence of Gender in the Copenhagen School," *Millennium*, 29(2): 285–306, 2000.

[23] Derian. D.J. "The Value of Security: Hobbes, Marx, Nietzsche, and Baudrillard." In D. Campbell and M. Dillon (eds.), *The Political Subject of Violence*. Manchester University Press, Manchester, 1993.

[24] B. Buzan, O. Wyer, J.D. Wilde and O. Waever. *Security: A New Framework for Analysis*, p. 27. Lynne Rienner Publishers, Inc., Boulder, 1997.

[25] B. Buzan, O. Wyer, J.D. Wilde and O. Waever. *Security: A New Framework for Analysis*, especially pp. 23–25. Lynne Rienner Publishers, Inc., Boulder, 1997.

ness-as-usual'' including: (1) reduced restraints on government powers, frequently manifested in the curtailment of civil liberties. In the USA PATRIOT Act, for example, some have seen a worrying move to extend wide-ranging, less-restricted powers of national security agencies to the domestic realm as necessary for the fight against terrorism; (2) breaks from normal democratic procedure, including government secrecy normally not tolerated by citizens (this, too, has seen in the period following the September 11 attacks.)[26] Other breaks occur when, in the name of security, officials circumvent normal principles of justice, such as routine use of racial profiling, officially forbidden in domestic law enforcement;[27] (3) steep incremental funding for security agencies and infrastructures. Although questioned in some quarters, most public leaders and citizens seem to accept national defense as having a high (perhaps the highest) priority claim on collective resources, even channeling resources away from other valued public goals.[28]

## Implications for computer security

I began the paper by claiming that distinct conceptions of computer security could steer practical efforts along diverging paths, spelling tension in future political and technical decision-making. How this tension will resolve is not clear, though our survey has illustrated support for both conceptions in the voices of political leaders, technical experts, industry lobbyists, heads of security agencies, and the media.[29] Moves to securitize are clearly evident but not endorsed by a critical enough mass to outweigh competing conceptions.[30] In the concluding sections of the paper, the goal is not to settle the question which of technical computer security or cyber-security (and securitization) prevails, or will prevail in conceptualizing online threat (a great deal more empirical study would be needed) but briefly to outline the distinct futures we face if one or other does.

To map out the possibilities, consider a hypothetical neighborhood that has experienced a sharp rise in break-ins and household burglaries. Gathered to discuss security strategies, worried residents are split between two alternatives. In strategy A, public funds will fit each household with state-of-the-art locks, motion-detection systems, and burglar alarms linked directly to the local police station. Residents would also subscribe to a neighborhood watch program. In strategy B, public law enforcement agencies will be brought in to install floodlights in all public spaces, as well as centrally managed networked surveillance cameras fitted with facial recognition systems. Checkpoints staffed with private security

[26] For more on the subject of government secrecy, see Rotenberg M. ''Privacy and Secrecy after September 11.'' In *Bombs and Bandwidth* (Latham R. ed.) (The New Press, 2003), pp. 132–142.

[27] The point is derived from Will Kymlika, ''Justice and Security in the Accommodation of Minority Nationalism, Comparing East and West.'' Draft paper presented at Princeton University, 2001, especially pp. 16–21.

[28] For a critical discussion of this practice, see Goodin (1982), *Political Theory and Public Policy*, Chicago: The University of Chicago Press, Chapter 11, ''The Priority of Defense.''

[29] A similar connection but with motion in the other direction is pointed out by Birnhak and Elkin-Koren in an important paper on the ways security concerns have allowed the state to re-enter governance of the Net by collaborating with private actors (Birnhack D. M. and Elkin-Koren N. (2003)), ''The Invisible Handshake: The Reemergence of the State in the Digital Envitonment'', 8 *Virginia J. of L. & Tech*, 6. Attorney General John Ashcroft stressed the possible dangers to the society as a result of intellectual property infringement: ''Intellectual property theft is a clear danger to our economy and the health, safety, and security of the American people.'' Attorney General John Ashcroft, Announces Recommendations of The Justice Department's Intellectual Property Task Force, October 12, 2004. available at: [http://www.usdoj.gov/criminal/cybercrime/AshcroftIPTF.htm]. The possible relation between security and intellectual property theft was recognized in the task force report itself: ''... those who benefit most from intellectual property theft are criminals, and alarmingly, criminal organizations with possible ties to terrorism.'' See U.S. Department of Justice, *Report of the Department of Justice's Task Force on intellectual property*, October 2004, p. 7. available at: [http://www.usdoj.gov/criminal/cybercrime/IPTaskForceReport.pdf].

[30] Evidence of disunity comes, for example, from the Federal District Court in Manhattan ruling in *Doe v. Ashcroft*, 334 F. Supp 2d, 471 (2004), striking down, on constitutional grounds, a section of the USA PATRIOT Act that would have allowed government security agencies to subpoena personal information from Internet Service Providers without having to obtain a court order.

officers as well as, occasionally, police will be posted at key intersections.[31] While common sense tells us that A and B will both reduce the incidence of crime in the neighborhood, their designs for doing so are quite distinct.[32]

Applying this case to the context of computers and information networks, we find strategy A closer to the heart of technical computer security; it seeks to protect individuals by fortifying individual (or institutional) nodes on the network. It is less concerned with identifying and stopping attackers before they act and more focused on strengthening protections for potential targets of such attacks as may occur. This approach is similar to recommendations from a February 2003 report of the Bush administration, *The National Strategy to Secure Cyberspace*, which seeks to reduce weaknesses in protocols and applications that open end-users to destructive attacks such as viruses and worms, destructive mini-applications, and denial of service. Similarly, in a statement to a Subcommittee of the U.S. Senate, Amit Yoran, Director of the National Cyber Security Division of the Department of Homeland Security, recommends a "threat-independent" approach focused on reducing vulnerabilities rather than on identifying and undermining specific threats.[33] His argument, which is compatible with recommendations of *The National Strategy to Secure Cyberspace,* is that limited resources would be more effectively applied to shoring up vulnerabilities and known system weaknesses.[34] How to reduce vulnerability is a technical question which leads us back to precepts of technical computer security.

Strategy B, with its checkpoints and surveillance, differs from A in at least two respects: one, in casting all passers-by within a net of suspicion, the other, in vesting greater control in the hands of centralized authorities. These moves are compatible with securitization because, by anticipating dire and imminent attack, it makes sense to seek to stop it before it occurs. This is best done by knowing who everyone is and what they are doing. Technical barricades that prevent access by all but authorized entities are the online equivalents of checkpoints. Although authorization *could* be tied to qualifying but non-identifying features, such as reputation and account status, the trend seems to be toward full identification, for example, in the energetic embrace of biometric identification, flight passenger profiling systems, and even road toll systems in the U.S. such as EZ Pass. Floodlit, biometric-enhanced video surveillance find parallels online in mechanisms that monitor and filter information flows such DCS1000 (previously Carnivore), intrusion detection systems monitoring unusual activity, and regulation to extend the CALEA (Communications Assistance for Law Enforcement Act) requirement of ability to tap phone lines to voice-over IP. The USA PATRIOT Act gives law enforcement and security personnel greater powers to scrutinize online postings and communications.[35] Also predicted by the model of securitization are the persistent calls for large increases in funding for computer security, security research, and cyber-crime units.[36]

In the case of the neighborhood, as in the case of computers and networks, the choice is difficult partly because it is contingent not only on facts of the matter, which are not all that well understood, but also on preferences and values, which are contested. A neighborhood resident, enthusiastic about the virtues of both A and B, might suggest doing both (surely there's no such thing as too much security). The problem with this solution is that even if it were affordable, it overlooks inherent incompatibilities in underlying values. In the online context, the incompatibilities between the parallels to strategies A and B are not only so in the dimension of values but also materially. Technical computer security demands protection for individuals from a variety of harms including breaches of confidentiality and anonymity and a chilling of speech, action, and association. Strategies of type B involve scrutiny, individual

[31] Obviously, these are paradigmatic and designed to illustrate alternatives at two ends of a spectrum which offers many variations in between.

[32] Discussions with Ed Felten greatly influenced the conception of this example.

[33] Statement by Amit Yoran, Director National Cyber Security Division Department of Homeland Security, before the U.S. Senate Committee on the Judiciary Subcommittee on Terrorism, Technology, and Homeland Security, February 24, 2004.

[34] The National Strategy to Secure Cyberspace, Bush Administration, final draft released February 14, 2003 (Available at: http://www.whitehouse.gov/pcipb/, November 24, 2004).

[35] E. Lipton and E. Lightblau, "Online and Even Near Home, a New Front Is Opening in the Global Terror Battle," *The New York Times*, September 23, 2004, A12.

[36] See for example the CIA and National Science Foundation joint project "Approaches to Combat Terrorism: Opportunities for Basic Research," aimed at finding ways to monitor on-line chat rooms. For more information about this project and additional ones visit EPIC website at: http://www.epic.org/privacy/wiretap/nsf_release.html. See also the "EFF Analysis of the Cyber Security Enhancement Act," available at: http://www.eff.org/Privacy/Surveillance/?f=20020802_eff_csea_analysis.html.

accountability, transparency, and identifiability which often are antithetical to the variety of individual liberties and self-determined choices protected in the alternative.

The considerations laid out above follow well-trodden paths in the theory and practice of politics, which in liberal democracies have resulted in familiar compromises such as rule-bound procedures for criminal investigation, prosecution, punishment, and governance generally. These issues extend well beyond the scope of this paper; our business here is merely to point out that design specifications for computer security may embody commitments to one understanding – technical computer security focused on the "ordinary" security of individuals – or another – cyber-security responding to threats that have been securitized.

If the securitization of online threats succeeds, the former might seem "too little, too late." But the extraordinary responses that securitization allows pose dangers of a different kind. By removing from individuals the cover of anonymity and confidentiality, and investing governmental and other authorities with greater power and discretion over their online activities, we expose their vulnerability to tyranny of corrupt officials or simply excessive control of over-reaching authorities. Strategies of type B work in the face of dire and urgent threats, among other things, by suppressing harmful attacks, but they open a population to the risk that suppression extends beyond its target in ways mentioned above. Moves to securitize should therefore be carefully scrutinized.

## Is securitization warranted?

In developing their framework, Buzan and Waever are preoccupied primarily with the construction of securitization and not with the question a realist might ask: when is securitization legitimate, or warranted? They do not altogether ignore this question, recommending as a general rule that a society (nation, state, etc.) set a high threshold for accepting securitizing moves on the grounds that removing important issues from the realm of public deliberation, and allowing leaders to work outside the constraints of cherished political principles, has potentially high costs.[37] I would like to give their recommendation greater specificity, perhaps pushing beyond the boundaries that a constructivist might set. To answer the question of the warrant of securitization, guided by the precepts of the framework and a skeptical stance, we must set about discovering how dire, how imminent, how total the presumed threats are. We should question the appropriateness of the proposed measures and their proportionality to the threats.

In the context of computer and online security the question of how dire and imminent the threats are calls for data and analysis that is not readily available to the broader public. One reason for the difficulty is that although many of the top technical security experts (computer scientists and engineers) pursue research into technical vulnerabilities, that is the *possibilities* for attack and damage, they do not seem to have a holistic of picture of their *probabilities*, the general incidence, of that actual damage. This calls for more than technical analytic understanding. Sporadic stories of attacks in publicly available sources and even the direct experience by ordinary users are insufficient for drawing wise conclusions. Certainly, they do not constitute sufficient basis for choosing between the models constructed by technical security and cyber-security, respectively. Those who follow these issues also learn that much is withheld or simply not known, and estimates of damage strategically either wildly exaggerated or understated.

In looking for supporting evidence for one of the two competing conceptions, a problem beyond the scarcity of relevant data and analysis is how to interpret (or read the meaning of) attacks that we do hear about. A virus attack on the Internet that corrupts thousands of computer systems, interpreted within the technical security model, is presented as a criminal attack against thousands of individuals and is the business of domestic law enforcement, constrained by relevant protocols of investigation, arrest, and so forth. This same attack, within the cyber-security model, may be construed as an attack against the nation, and count as evidence for securitization. The importance of meaning attributed to an event was evident in the minutes and hours following the attacks on the World Trade Center – conceived not as crimes against the many *individuals* killed and injured but as a transgression against the U.S. – not by particular individuals, but by the terror organizations and nations constituting the "axis of evil." Corporate owners of intellectual property have been particularly adept at reading broad meanings into unauthorized uses and distribution of copyrighted materials, lobbying with relative success to pose these activities as deeply threatening not only to them but the U.S. economy. Their efforts have paid off in predictable ways (according to the Copenhagen School), namely measures that many legal scholars argue are

[37] B. Buzan, O. Wyer, J.D. Wilde and O. Waever. *Security: A New Framework for Analysis*, discussion on pp. 29–30. Lynne Rienner Publishers, Inc., Boulder, 1997.

extraordinary, including quite general attacks on P2P file-sharing, which they pose as a threat to law and order.[38] These lobbies have also successfully achieved incremental appropriations of government funds for law enforcement efforts to stem unauthorized exchanges, such as a $32 million increase in spending in 2001 for FBI cyber-crime units and equipment.[39] Further, there has been significant ramping up of punishment regimes.

## Conclusion

This paper has argued that the way we conceptualize values can influence the shape of technical design and related public policy. In the research, design, development, and regulation of computer security, it is clear that strong commitments to the underlying value of security motivates much of its attraction and public support. But what I have tried to show is that at least two quite distinct and incompatible conceptions of security vie for public and expert support, and that which of the two ultimately dominates will make a difference for computerized, networked individuals and societies. How these differences play out through law, policy, and budget appropriations is important but this paper has sought particularly to indicate the potential of the two conceptions for shaping technical design. The reason for this focus is not that the realm of system design and development is more important, but because it is all too often neglected as a site for resolving political and ethical conflict. Further, once standards are adopted and constraints and affordances built, technical systems are less tractable than other forms of policy resolution.[40]

In laying out some of differences between the two conceptions of security, I have tried to show what is at stake in the selection of one over the other. If those who subscribe to a conception of security as cybersecurity are right, particularly if the magnitude of threat is as great as those on the extremes claim, then an extraordinary response (strategy B in the hypothetical neighborhood) is warranted despite its chilling effects. In the context of airports, we seem to have accepted such conditions: virtually ubiquitous informational and visual surveillance with highly controlled patterns of movement.[41] Presumably, nuclear power plants and high-security prisons limit freedom of action in similar ways, and justifiably so.

I am inclined to resist a move to frame computers and networked information and communications systems in these ways, as so dangerous that they warrant extraordinary treatment of this kind. This inclination has less to do with efficacy than purpose. As long as we value our networked information infrastructure for its contribution to public communication, community, political organization, association, production and distribution of information and artistic creation, its security is best pursued under the conception I called "technical computer security." Just as the residents of our hypothetical neighborhood might agree that improvements in safety would be greater with strategy B, they may nevertheless choose A because they prefer the type of neighborhood that would follow as a result. Similarly, securitization might makes the Net safer but at the expense of its core purpose as a realm of public exchange. It makes no sense to make security the paramount value when this essential purpose is undermined. Aquinas recognizes this point when he advises, "Hence a captain does not intend as a last end, the preservation of the ship entrusted to him, since a ship is ordained to something else as its end, viz. to navigation;"[42] or in Goodin's paraphrase, "...if the highest aim of the captain were to preserve his ship, he would keep it in port forever."[43]

[38] Digital Millennium Copyright Act of 1998 (DMCA), Pub. L. No. 105–304, 112 Stat. 2860, Codified as 17 U.S.C. §§1201–1205; for commentary review see: Litman J. (1994), "The Exclusive Right to Read," 13 *Cardozo Arts & Ent. L. J.*, 29; Samuelson P. (1999), "Intellectual Property And The Digital Economy: Why The Anti-Circumvention Regulations Need To Be Revised," 14 *Berkeley Tech. L. J.* 519; also, see the legislation: S. 2560, The International Inducement of Copyright Infringement Act of 2004 (The INDUCE Act)., presently "on hold".

[39] "House Gives Final Approval to FY 2002 Commerce, Justice, State and Judiciary Spending Bill," *CJIS Group News* (November 14, 2001) available at: [http://www.cjis-group.com/aboutCJIS/newsBudget111401.cfm]

[40] L. Winner. *Do Artifacts Have Politics? The Whale and the Reactor: A Search for Limits in an Age of High Technology*. University of Chicago Press, Chicago, 1986.

[41] See for example the attempt to create passenger profiling as part of the Secure Flight passenger prescreening program. The Transportation Security Administration has ordered airlines to turn over a month's worth of passenger data, which will allow the creation of passenger profiling. For more information about this step and the attempt to prevent such profiling in the name of privacy right, visit the Electronic Privacy Information Center (EPIC) website, available at: [http://www.epic.org/privacy/airtravel/profiling.html].

[42] Aquinas, *Summa Theologica*, Part I of II, Question 2, Article 5.

[43] Robert, G. *Political Theory and Public Policy*, p. 233. The University of Chicago Press, Chicago, 1982.