Theoretical Background to Risk and Security in the Information Age

Learning Object Description

Why is information and communications technology (ICT) considered a security risk at a national level, even though cyber-threat scenarios have not materialized so far? This is the crucial question this learning object addresses. It introduces you to the research field of security studies and highlights some of the most important and most recent approaches to security. In particular, the key concepts of securitization and threat framing are briefly introduced. To conclude the learning object, the theory of threat framing is applied to cyber-threats.

Learning Object Objectives

The aim of this learning object is to explain why ICT has become such a pressing issue for national security specialists. By means of an introduction to international relations (IR) theories, you will get to know the key concepts of securitization and of threat framing, and you will be able to apply these to cyber-threats. You will learn about why ICT-related risks are so important to national security specialists, even though no major cyber-incident has occurred so far.

Introduction

Imagine the following scenarios:

Emergency response systems collapse as truck explodes

A truck carrying a huge bomb races towards the main entrance of a city center rail station at rush hour, just as a computer whiz hacks into the emergency response telephone network. There is a huge blast. With the communications system out of action, police and rescue units are paralyzed. Emergency teams lose precious minutes attending to the scene, and the number of dead and injured climbs.

12-year old hacks Roosevelt Dam control systems

A 12-year old hacks the system that runs the Roosevelt Dam, near Phoenix, Arizona, which contains nearly 500 trillion gallons of water. The cities Mesa and Tempe are downstream, with a combined population of 1 million – the kid accidentally opens the floodgates: 100'000 people die in the torrents of the rampant Salt River.

Computer virus causes massive power cuts

A virus deliberately introduced into the software system of a power station by a terrorist group triggers a complete power loss that plunges a large part of three European countries into darkness. About 168 million people are affected. Power cannot be restored for up to four days in some parts of the affected region. The outage of traffic lights leads to chaos. Millions of car drivers are left without fuel, because petrol station pumps run on electricity. The water supply is seriously compromised; the interruption lasts for days. Both the telephone network and mobile phones are operating, although services are in a critical state. Most Internet providers have to shut down their servers, because they are not able to switch to their diesel-driven backup generators. The estimated financial loss is about €970 million. A great number of people die as a result of the power cuts.

Frightening? We all know from daily experience that computer applications – from our word processing program to business billing systems – are error-prone and break down frequently. Fixing the bugs cost time and money and can cause a lot of annoyance, but this is not usually a serious issue for national security. However, the above scenarios describe incidents with

severe consequences and explain why cyber-threats are treated as a national security issue in many countries. This learning object deals with ICT risks with regard to security policy and investigates the question of why and how ICT-related security risks have become so important to national security policy specialists.

To get started, have a go at the following exercise, and try to find out which of the three above-mentioned events really happened.

Question 1

Decide which of the stories are completely true, partly true, or completely made up:

Story	**List of matchables**
Emergency response systems collapse as truck explodes	Completely true
12-year old hacks Roosevelt Dam control systems	Partly true
Computer virus causes massive power cuts	Completely made up

Cyber-Threats: Real Danger or Panic-Mongering?

The misreported dam-incident can serve as a metaphor for today's debate about the vulnerability of networked societies to cyber-threats. While governments and the media repeatedly distribute information about cyber-threats, real cyber-attacks resulting in deaths and injuries remain largely the stuff of Hollywood movies or conspiracy theory.

Cyber-attacks and cyber-incidents are indisputably a costly affair for the business community, and they cause major inconveniences. In the last few years, such incidents have cost billions of dollars in lost intellectual property, maintenance and repair, lost revenue, and expenditures for increased security. Further, cyber-attacks might also reduce the public's confidence in the safety of Internet transactions and e-commerce, damaging corporate reputations and reducing the efficiency of the economy.

However, controversy remains high about whether or not the Internet and other information infrastructures pose a true national security threat: If the damage caused by a cyber-attack does not rise above the threshold of the routine disruptions that every economy experiences, it does not pose an immediate or significant risk to national security. None of the larger and smaller disruptive cyber-incidents that we have experienced in the past few of years has had an impact that has genuinely threatened society.

The question arises: Is it possible that the discussion about threats and vulnerabilities related to the information age is pure panic-mongering? Some observations seem to support this view:

- On the whole, and with regards to the amount of activity that we know occurs, our modern, technology-based societies seem to function exceptionally well, and the technological environment has been surprisingly stable, even though many disruptions of various extents, both accidental or caused by humans, occur every day.
- Many aspects of the threat are unsubstantiated; or rather, there is insufficient empirical data for us to evaluate the severity of the risk. Due to a lack of experience, statements about the scope of the danger are often purely speculative. Currently, there are no consolidated statistics regarding computer-based threats, and there are no incident rates. Detection technology is known to be of limited use, making it difficult to define the scope and degree of the threat. As a result, there are a number of uncertainties in any given threat assessment. Qualitative information remains anecdotal, making it difficult for the intelligence and enforcement community to carry out an effective analysis of the changing nature of the threat and the degree of the risk.

Experts widely disagree about how likely cyber-doom scenarios are and how serious a threat such scenarios pose. Most official publications are not only very vague about the actual level of threat, but they also leave cyber-threats shrouded in a mist of speculation. This is not helped by poor definitions and careless use of terminology by many government officials, which has caused the issue to become exaggerated and subject to dramatization and alarmist warnings.

However, the hype surrounding cyber-threats has created a growing number of more cautious voices that try to be more specific in their estimates of the threat. Many of the more technically astute political advisors and commentators argue that bureaucracies like militaries

and intelligence agencies, as well as many terrorist groups, are incapable of acquiring the skills and means to cripple ICT systems and have written about the practical difficulties of carrying out a serious cyber-attack. They also say that although electronic intrusions may damage infrastructures and even threaten physical damage, it is extremely difficult to take control of those systems from the outside. Such action would require a great deal of specialized knowledge, and the perpetrators would have to overcome non-computerized fail-safe measures.

Other observers point to the fact that combating cyber-threats has become a highly politicized issue – and a lucrative one: An entire industry has emerged to deal with the threat.

Security budgets soared in 2003

Read a news story from "The Register" about the growing market for ICT security products.

Hyperlink to http://www.theregister.co.uk/2004/04/06/datamonitor_security2003/

Exercise

Before continuing, please complete the exercise below.

Question 2

Which of the following statements is correct?

- ☐ The execution of a serious cyber-attack would require the attackers to overcome some serious practical difficulties.
- ☐ So far, real cyber-attacks resulting in deaths and injuries remain largely the stuff of Hollywood movies or conspiracy theory.
- ☐ Controversy remains high about whether or not the Internet and other information infrastructures pose a true national security threat.
- ☐ Combating cyber-threats has become a highly politicized and lucrative issue, and an entire industry has grown around it.
- ☐ Bureaucracies like militaries and intelligence agencies, as well as many terrorist groups, face a range of difficulties when it comes to acquiring the skills needed to become successful hackers.

- ☐ Statements on the extent of the danger from cyber-threats are often purely speculative.
- ☐ Some experts maintain that our modern, technology-based societies function exceptionally well, and the technological environment has been surprisingly stable.

In the next section, we turn to the issue of why cyber-threats have nevertheless become a high priority for national security experts.

Cyber-Threats on the National Security Agenda

Even those experts most critical of the hype surrounding cyber-threats are unwilling to dismiss the threat completely:

- Most of them believe that even though the threat may be exaggerated and manipulated by some, it cannot be ignored: Future technological development and the dynamic change of the capabilities of potential adversaries is rapid and difficult to assess. Therefore, even though there have been no truly threatening incidents so far, experts seem unable to decide whether cyber-doom is fact or fiction, or, since they are unable to dismiss it completely, how long it will remain fiction.
- The ongoing debate has put considerable pressure on decision makers. For many governments, the necessary line of action has been clear: They consider the threat to national security to be real, and have drafted or implemented steps for countering it.

Thus, the perception that cyber-doom is a threat has become established, persists, and has proliferated globally, gaining a high priority among national security experts – even though it has little, or, some would argue, no, connection to real world occurrences. Further, many governments spend considerable amounts of money on counter-measures against a threat that has not materialized so far.

This observation raises some interesting questions, from a security studies perspective:

- Why and how does a threat that has little or no link to real world occurrences become such an important issue for the security policy specialists of so many countries?

- Are cyber-threats marked by specific characteristics that have made the issue so important?

To answer these questions, we will now link the cyber-threats debate to security studies, a research field traditionally seen as a sub-field of international relations (IR).

Transitions in Security Studies

The field of security studies has undergone significant changes in recent years, brought on by two major developments.

The first development has its origins in the late 1970s, when the publication of Power and Interdependence: World Politics in Transition by Robert O. Keohane and Joseph Nye brought about a new understanding of the global system. Keohane and Nye challenged the traditional theory, which saw the global system as a series of interactions between unitary states concerned primarily with national security, which in turn was defined in military terms. Instead, they proposed that the modern global system was characterized by multiple issue areas, the breakdown of hierarchies in particular issue areas, the declining usefulness of force, the importance of international regimes, and the fragmentation of authority in each state. Instead of referring to international "relations", Keohane and Nye referred to international "interactions". Their book ushered in a "broadening and deepening" of the concept of security (Krause and Williams, 1997).

Reference

Keohane, Robert O. and Joseph S. Nye (1977). *Power and Interdependence World Politics in Transition.* Boston: Little, Brown and Company.

Reference

Krause, Keith and Michael Williams (eds.) (1997). *Critical Security Studies Concepts and Cases.* Minneapolis: University of Minnesota Press.

The broadening of the concept of security means that we now add economic, societal, political, and environmental risks to the classically dominant military threats; the debate focuses on what threats and issues should be studied. The deepening of security means that we now add more actors to our analysis of security; these include individuals, the ecological system, and communities. This broader understanding of security is a result of the major reorientation of security policy initiated when the Cold War ended. As old security problems lost significance, governments demanded analyses of policy proposals and of the emerging and largely unfamiliar new security landscape. Experts and analysts who previously had monitored well-known problems were now tasked with finding out what the new security problems were and with identifying new challenges and problems. Governments turned to advisors, specialists, analysts, and researchers and gave them the freedom and opportunity to identify "new" threats that they considered of vital importance to national security.

The second development in the field of security studies relates to the theories used to analyze security issues. In the next section, we will look at the debate between positivist and post-positivist theory.

Exercise

Before continuing, please complete the exercise below.

Question 3

Describe in your own words what the "broadening and deepening" of the concept of security has entailed:

Positivist and Post-Positivist Security Studies

There are many different strands in post-positivism, as practiced in security studies. However, all post-positivist theories express dissatisfaction with the positivist mindset, which takes an "objective and unproblematic" (McSweeney, 1999) approach to the theory of security. This approach is marked by the assumptions that there is a real world out there and that this world can be measured and analyzed.

Post-positivists, however, take a subjective approach to knowledge, suggesting that the production of knowledge is contested, i.e., it is not given and it is problematic; or they believe the world is socially constructed, i.e. not an empirically identifiable given; or they subscribe to both views.

The following are the main strands of post-positivism:

Constructivists

This group believes that the world is the product of our social interaction, which can be measured and analyzed by scientific means. Constructivism is primarily interested in the notion that security is what states (and other key actors) make of it, meaning that security is inter-subjectively constructed. We will apply the constructivist perspective to the cyber-threats debate below.

Critical Security Studies

This strand is the product of the belief that there is a world out there which cannot be easily measured and analyzed because of the contested nature of the production of knowledge. Therefore, critical theory is specifically concerned with the way knowledge is produced in the field of security, and scholars of this school primarily hold that security is produced to serve the (various) purposes and agendas of actors and states.

Postmodern Security Studies

Postmodernists apply the approaches of both the IR constructivists and the critical theorists: Postmodernism is based on the belief that the world is the product of our social interactions or performances and cannot be easily measured and analyzed, because of the contested nature of knowledge production. This strand is characterized by diversity.

When we apply a positivist approach to a security threat, certain views about the nature of a security threat are given. Post-positivist approaches look at how, when, and with what consequences political actors frame something – anything – as a matter of security, and they put much emphasis on political language and on the implications this language has for political agenda-setting and political relations.

In the following section, we will take a constructivist approach, as such an approach allows us to understand and explain the hype surrounding the cyber-issue.

Securitization and Threat Framing

The many new security issues that emerged with the end of the Cold War led experts to ask how and why certain new threats gained such prominence and to try to identify the key factors that led to the emergence of these new threats.

The so-called "Copenhagen school" of security around Barry Buzan and Ole Wæver has developed an approach that focuses on the process of bringing an issue from a politicized or non-politicized stage into the security domain. This process is called securitization. The process of securitization is seen as a socially constructed, contextual "speech act", meaning that by uttering "security", or another term expressing the need for exceptional measures, a state-representative moves a particular issue into the security realm and claims extraordinary means to prevent it or deal with it.

Ultimately, this means that an issue becomes a security issue not necessarily because there is a real existential threat, but because the issue has been successfully presented and become established as a threat by key actors in the political arena. Thus, securitization studies aim to gain an understanding of who securitizes (the actor) what issues (the threat subject) for whom (the referent object) why (the intentions and purposes) with what results (the outcome) and under what conditions (the structure and/or institutions).

Frame theory is rooted in linguistic studies of interactions and illustrates the ways in which shared assumptions and meanings shape the interpretation of a given event. Put simply, framing can be understood as the subtle selection of certain aspects of an issue as a means of eliciting a specific response; the way an issue is framed determines who is considered responsible for causing a particular problem and who is considered responsible for solving it.

The way an issue is framed also indicates which solutions are deemed suitable and effective. Threat framing, in particular, refers to the process by which particular agents develop specific interpretive schemas about what counts as a threat or a risk, how to respond to this threat, and who is responsible for it.

Exercises

Before continuing, please complete the exercises below.

Question 4

Which are the common features of post-positivist security studies?

- ☐ All post-positive theories are interested in the notion that security is whatever states make of it.
- ☐ All post-positive theories express dissatisfaction with the positivist mindset.
- ☐ All post-positive theories raise questions about the role of positivism in the study of security from a variety of viewpoints.
- ☐ Contrary to positivist approaches, in post-positive theory it matters how, when, and with what consequences political actors frame something as a security issue.

Question 5

Which statements apply to the term “securitization”?

- ☐ Securitization is a theoretical framework based on the notion that security is inter-subjectively constructed in IR.
- ☐ Securitization is a theoretical approach that focuses on the process of bringing an issue from a politicized or non-politicized stage into the security domain.
- ☐ Securitization studies aim to understand how “new” threats make their way on to national security agendas.
- ☐ Securitization means that an issue can become a security issue even though it may not pose a real existential threat.

Let us come back to the cyber-threats issue and analyze the issue from a constructivist security studies perspective. The next section will identify that which appears to be threatening (the subject of the threat image or threat subject), what is perceived as being threatened (the object of the threat image or referent object), and that object's general characteristics. That way we can identify key aspects of the cyber-threat frame in order to find out why this fear is so persistent, even though it seemingly remains an unsubstantiated threat.

Cyber-Threat Frames

Is there something about the substance of information and ICT that has brought them to the attention of security experts and government officials? In general, conceptions of cyber-threats are very broad and also very vague, both in terms of what or who is seen as the threat, and of what or who is seen as being threatened.

Nevertheless, when we analyze the cyber-threat issue from the perspective of the constructivist school, especially that of the Copenhagen school, we find the following common features in the framing of cyber-threats:

Referent object

Cyber-threats are ultimately seen as a threat to society's core values, particularly to national security, and to the economic and social well-being of a nation. Therefore, they are inevitably presented as a national security issue and are "securitized". Reasons given for the perception of cyber-threats as a danger are vulnerabilities caused by the dependence of society on the information and communication infrastructure, on the one hand, and ever-more complex interdependencies between infrastructures, on the other.

Threat subject

Cyber-attacks can be undertaken in many ways, potentially by anyone with a computer connected to the Internet, and for purposes including juvenile hacking, organized crime, political activism, and strategic warfare. Via the Internet, hacking tools can be easily downloaded and have become both more sophisticated and more user-friendly.

Characteristics

Cyber-threats are typically seen as elusive and complex. Due to the global nature of information networks, attacks can be launched from anywhere in the world, and discovering their origin, if they are detected at all, remains a major difficulty. Unlike traditional security threats, which can be analyzed in terms of actors, intentions, and capabilities, cyber-threats cannot easily be broken down into their constituents and are therefore very difficult to monitor, analyze, and counteract. Hence, adversaries are typically seen as operating in loosely organized networks consisting of relatively independent nodes of individuals, groups, organizations, or states, capable of assembling and dispersing quickly, even a long time before an attack has been discovered.

The introduction of numerous non-state enemies as threat subjects dissolves the distinction between internal and external threats and between the private and public spheres of action. The opening up of this very wide range of potential adversaries can emphasize vulnerability, uncertainty, and insecurity. In addition, cyber-threats by their very nature dissolve perceived boundaries between the civil and military spheres, and between peace and war, again leading to increased uncertainty and insecurity.

Further, the vulnerability of the ICT infrastructure and the dependence of society on that infrastructure arise not only from the fact that events occur sporadically, but also from a general and increasing inherent weakness within the emerging network society, and this is a major reason for securitization. Cyber-threats, therefore, seem to be an unmanageable risk that invokes a maximum of fear. Viewed in relation to the magnitude of the referent object – society as a whole – there seems to be no other option than to establish cyber-threats as an issue for national security, which would justify the use of extraordinary measures to deal with them.

Reference

If you want to read more about securitization of ICT-related issues, read the following article: Eriksson, Johan (2001). "Cyberplagues, ICT, and Security Threat Politics in the Information Age." *Journal of Contingencies and Crisis Management* 9, 4 December 2001, 211-222.

The Reality of Fiction

We have established that it is impossible, at present, to conclude whether cyber-threats are fact or fiction from an analyst's viewpoint – and the approach to the issue that we have looked at in this lesson does not help us to determine whether cyber-threats are fact or fiction or, if we do, in fact, view them as a fiction, how long they will remain a fiction.

But what does this mean for the decision maker? There is an obvious rift between theory and practice: Cyber-threats have not (yet) become a reality, and there is a lot of uncertainty about the future development of this threat, especially as long as the capabilities of possible adversaries remain unknown. Nevertheless, governments around the world still act as though cyber-threats were a reality. This basically means that, in practice, it does not matter whether a threat is real or not. What matters is that decision makers consider cyber-attacks a real threat and act accordingly.

Even though the analysis of threat frames does not help to determine whether or not cyber-attacks pose a threat, analyses of potential cyber-threats can at least show us why certain countermeasures are considered more suitable than others. For example, we see that the types of institutional solutions vary according to whether a state considers either other states or, rather, various non-state actors as a threat subject: If the threat subject is perceived to be state actors, a state will tend to focus on strategic questions and military responses; when the threat is perceived to originate mainly from sub-state actors, a state will tend to focus primarily on by law enforcement responses.

However, we should ask ourselves how useful it is to include cyber-threats on the national security agenda. Do cyber-threats really deserve the attention they are receiving, or could such prioritization be misguided? Events from the past couple of years suggest that computer network vulnerabilities are an increasingly serious problem for businesses, but the threat to national security seems exaggerated. As long as a cyber-attack does not cause damage beyond the routine disruptions that every economy experiences, it does not pose an immediate or significant risk to national security. However, the current threat frame is so persuasive that any attempt at desecuritization – the reverse process of securitization, i.e., the deprioritization of an issue as a national security threat – is most likely to fail.

Thus, since cyber-threats will most certainly remain on the national security agenda, decision makers should be careful not to incite cyber-angst, even if the threat itself cannot be

completely ignored. Decision makers seeking a prudent policy face the difficult task of balancing doomsday scenarios with uninformed complacency.

Exercise

Before continuing, please fill in the gaps in the text below.

Question 6

Is there something about the substance of information and ICT that has brought them to the attention of security experts? If we look at the cyber-threat discourse from a _____ perspective, we can _____ some key aspects of the cyber-threat frame that explain why this fear is so _____. The referent object, i.e. the object seen as under threat, is society's core _____. In addition, cyber-attacks may be launched by practically any state or non-state actor and from anywhere in the world. _____ theory does not explain whether cyber-threats are fact or fiction, but it does explain why decision makers consider the threat as real and why they are instituting certain countermeasures.

Summary

In this lesson, we looked at why ICT are considered a considerable threat to nation states, even though no major cyber-incident has occurred so far.

The following points are worth remembering:

- Discussions about ICT as a security issue vary between panic-mongering and serious attempts to understand the consequences of the rapid development of the technology and of the capabilities of potential adversaries.
- In order to understand why ICT have become a priority for national security specialists, we should consider research undertaken in the field of security studies, a sub-branch of IR.
- Until recently, positivism has been the dominant theory in security studies. Positivist approaches to security see threat images as "given" and "out there" and assume that real threats are directly reflected in security policy planning; thus, security policies are responses to objective threats and risks.
- Post-positivist approaches to security studies have a different definition of security and tackle a range of new questions. Post-positivist approaches focus on how, when, and with what consequences political actors frame something – anything – as a security issue. They place a strong emphasis on political language and the implications language has for political agenda-setting and political relations.
- The Copenhagen School analyzes the process through which an issue (politicized or non-politicized) becomes a security issue – a process called securitization.
- When we look at cyber-threats in terms of the process of securitization, we come to understand why the threat is tackled by policy makers as if it were a real threat.
- When cyber-threats are analyzed from a constructivist point of view, some key aspects of the cyber-threat frame become obvious, showing why the fear of ICT attacks persists, even though it is unsubstantiated.

- The referent object, i.e. the object against which cyber-threats are directed, is society's core values (i.e. particularly national security) and the economic and social well-being of a nation. The threat subject is cause for particular alarm, because cyber-attacks can be undertaken in innumerable ways, potentially by anyone with a computer connected to the Internet. Cyber-threats are typically seen as very elusive and complex.
- Analyses of the framing of cyber-threats show why cyber-threats are an unmanageable threat that invokes a maximum of fear. Viewed in relation to the magnitude of the referent object – society as a whole – there seems to be no other option than to establish cyber-threats as an issue for national security, which justifies the use of extraordinary measures to deal with them.
- It is impossible, at present, to conclude whether cyber-threats are fact or fiction from an analyst's viewpoint. Nevertheless, cyber-threat frames show why governments around the world act as though cyber-threats were a reality and explain the perception of cyber-threats as a national security issue.

Answers to the Exercises

Question 1

Decide which of the stories are completely true, partly true, or completely made up:

Story	**List of matchables**
Emergency response systems collapse as truck explodes	Completely made up
12-year old hacks Roosevelt Dam control systems	Partly true
Computer virus causes massive power cuts	Partly true

The first story is completely made up. The second one, however, is partly true. The Washington Post reported on 27 June 2002 that a 12-year-old hacker had broken into the computer system that controlled the floodgates of the Theodore Roosevelt Dam in Arizona in 1998. True, a hacker did break into the computers of an Arizona water facility, the Salt River Project, in the Phoenix area. But he was 27, not 12, and the incident occurred in 1994, not 1998. And while clearly trespassing in critical areas, the hacker never could have had control of any dams – leading investigators to conclude that no lives or property were ever at risk. The third story is partly made up but is inspired by the major blackouts in the US and Europe in 2003, which, however, were not caused by a hacker attack.

Question 2

The following statements are correct:

- ✓ The execution of a serious cyber-attack would require the attackers to overcome some serious practical difficulties.
- ✓ So far, real cyber-attacks resulting in deaths and injuries remain largely the stuff of Hollywood movies or conspiracy theory.
- ✓ Controversy remains high about whether or not the Internet and other information infrastructures pose a true national security threat.

- ✓ Combating cyber-threats has become a highly politicized and lucrative issue, and an entire industry has grown around it.
- ✓ Bureaucracies like militaries and intelligence agencies, as well as many terrorist groups, face a range of difficulties when it comes to acquiring the skills needed to become successful hackers.
- ✓ Statements on the extent of the danger from cyber-threats are often purely speculative.
- ✓ Some experts maintain that our modern, technology-based societies function exceptionally well, and the technological environment has been surprisingly stable.

In fact, all of the above statements are correct, and they summarize the main points of the previous section.

Question 3

Describe in your own words what the "broadening and deepening" of the concept of security has entailed:

Possible answer: *The broadening of subject of security means that economic, societal, political, and environmental risks were added to the classically dominant military threats, with the debate focusing on what threats and issues to study. The deepening of security was concerned with adding more actors, i.e. individuals, ecological system, communities, to the traditional state-centric units of analysis. This broader understanding of security is a result of the major reorientation of security policy that was initiated after end of the Cold War.*

Question 4

Which are the common features of post-positivist security studies?

- ✓ All post-positive theories express dissatisfaction with the positivist mindset.
- ✓ Contrary to positivist approaches, in post-positive theory it matters how, when, and with what consequences political actors frame something as a security issue.

Question 5

Which statements apply to the term "securitization"?

- ✓ Securitization is a theoretical approach that focuses on the process of bringing an issue from a politicized or non-politicized stage into the security domain.
- ✓ Securitization studies aim to understand how "new" threats make their way on to national security agendas.
- ✓ Securitization means that an issue can become a security issue even though it may not pose a real existential threat.

Question 6

Please fill in the gaps in the text below.

Is there something about the substance of information and ICT that has brought them to the attention of security experts? If we look at the cyber-threat discourse from a **constructivist** perspective, we can **identify** some key aspects of the cyber-threat frame that explain why this fear is so **persistent**. The referent object, i.e. the object seen as under threat, is society's core **values**. In addition, cyber-attacks may be launched by practically any state or non-state actor and from anywhere in the world. **Constructivist** theory does not explain whether cyber-threats are fact or fiction, but it does explain why decision makers consider the threat as real and why they are instituting certain countermeasures.

Bibliography

- Bendrath, Ralf (2001). "The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection." In: Wenger, Andreas (ed.). *The Internet and the Changing Face of International Relations and Security. Information & Security: An International Journal* 7 (2001), 80-103.
- Bendrath, Ralf (2003). "The American Cyber-Angst and the Real World – Any Link?" In: Robert Latham (ed.). *Bombs and Bandwidth: The Emerging Relationship Between IT and Security.* New York: The New Press, 49-73.
- Buzan, Barry, Ole Wæver, and Jaap de Wilde (1998). *Security: A New Framework for Analysis.* Rienner: Boulder.
- Czempiel, Ernst-Otto and James N. Rosenau (1989). *Global Changes and Theoretical Challenges: Approaches to World Politics for the 1990s.* Lexington [etc.]: Lexington Books.
- Eriksson, Johan (2001). "Cyberplagues, IT, and Security: Threat Politics in the Information Age." *Journal of Contingencies and Crisis Management* 9, 4 (December 2001), 211-222.
- Huysmans, Jef (1998a). "Security! What do you mean? From Concept to Thick Signifier." *European Journal of International Relations* 4, 2 (1998), 226-255.
- Keohane, Robert O. and Joseph S. Nye (1977). *Power and Interdependence: World Politics in Transition.* Boston: Little, Brown and Company.
- Krause, Keith and Michael Williams (eds.) (1997). *Critical Security Studies: Concepts and Cases.* Minneapolis: University of Minnesota Press.
- Lewis, James A. (2002). *Assessing the Risks of Cyber-Terrorism, Cyber War and Other Cyber Threats.* Center for Strategic and International Studies. URL http://www.csis.org/tech/0211_lewis.pdf.
- McSweeney, Bill (1999). *Security, Identity and Interests: A Sociology of International Relations.* Cambridge: Cambridge University Press.
- Reus-Smit, Chris (1996). "The Constructivist Turn: Critical Theory after the Cold War." Working Paper No. 1996/4. Canberra: Australian National University.
- Walt, Stephen M. (1991). "The Renaissance of Security Studies." *International Studies Quarterly* 35, 2 (1991), 211-239.
- Wendt, Alexander (2000). *Social Theory of International Politics.* Cambridge: Cambridge University Press.

ISN Run by CSS

This PDF was produced by the International Relations and Security Network (ISN) and is part of the e-learning course "Security in the Information Age". Last update 6 April 2005.