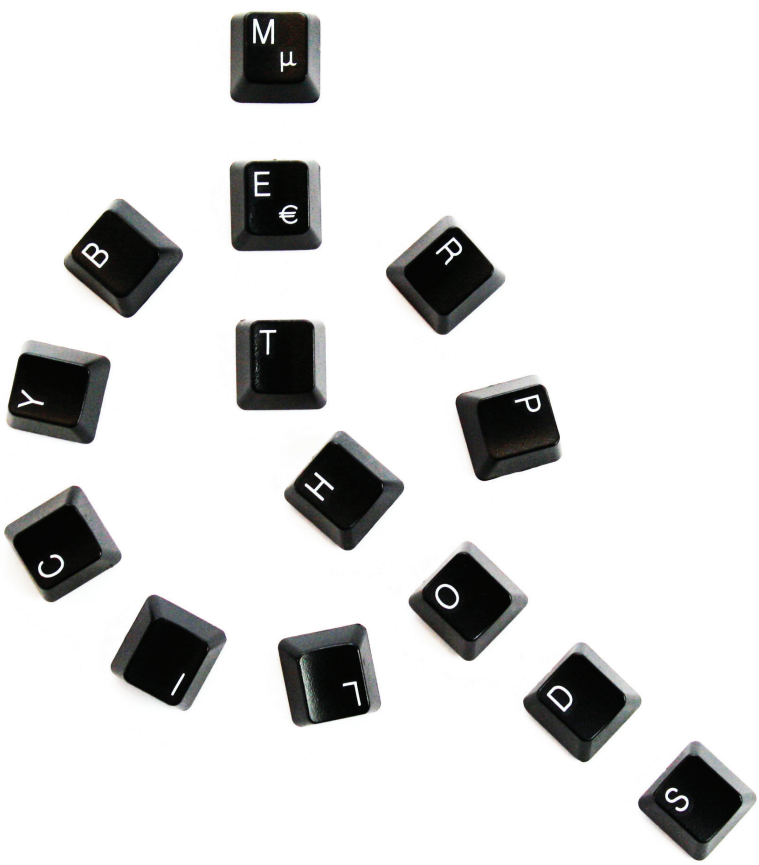
Security studies in the information age

A review of methods

ULRIK FRANKE, MIKAEL ERIKSSON,
JERKER HELLSTRÖM, STEVEN SAVAGE



FOI-R--3737--SE
ISSN 1650-1942 October 2013

Ulrik Franke, Mikael Eriksson, Jerker Hellström, Steven Savage

Security studies in the information age

A review of methods

Bild/Cover: FOI

Titel	Säkerhetsstudier i informationsåldern – en metodöversikt
Title	Security studies in the information age – a review of methods
Rapportnr/Report no	FOI-R--3737--SE
Månad/Month	Oktober/October
Utgivningsår/Year	2013
Antal sidor/Pages	58 p
ISSN	1650-1942
Kund/Customer	
Forskningsområde	8. Säkerhetspolitik
FoT-område	
Projektnr/Project no	I35404
Godkänd av/Approved by	Lars Höstbeck
Ansvarig avdelning	Informations- och aerosystem

Sammanfattning

Den här studien syftar till att illustrera hur många olika perspektiv och metoder som kan användas för att studera samspelet mellan å ena sidan informations- och kommunikationsteknik (IKT) och å andra sidan sociala och politiska skeenden. Rapporten täcker ett brett spektrum av vetenskapliga metoder, hämtade från samhällsvetenskap, datavetenskap, teknikvärdering och underrättelseanalys. Därutöver ingår två mer praktiskt orienterade avsnitt som täcker IKT-sanktioner respektive privatliv. Rapporten avslutas med en diskussion om hur olika metoder möter olika behov och förutsättningarna för att kombinera olika metoder i syfte att bättre belysa komplicerade fenomen.

Nyckelord: Säkerhet, informations- och kommunikationsteknik (IKT), samhällsvetenskap, teknikvärdering, underrättelseanalys, sanktioner, privatliv

Summary

The aim of this study is to illustrate the wealth of perspectives and methods for studying the interplay between information and communications technology (ICT) and social and political events. The report covers a broad range of available scientific and scholarly methods, from social science, computer science, technology assessment and intelligence analysis. In addition, two chapters are more practitioner-oriented, covering the areas of ICT sanctions and privacy. The report concludes with a discussion on how different methods suits different needs, and on the prospects for combining different methods to gain a better understanding of these complicated phenomena.

Keywords: Security studies, information and communications technology (ICT), social science, technology assessment, intelligence analysis, sanctions, privacy

Preface

This report has been produced within the National Security in the Information Society (SPIS) project at FOI. This project studies the complex interplay between our modern information society and national security, an evolving field that has attracted considerable attention in the wake of the Arab spring. The report is the last one in the course of the project, and brings closure to it by presenting the methodological variety in this interdisciplinary field of study.

The report has benefitted from the comments of Magnus Jändel and Gudrun Persson, who made valuable remarks as reviewers.

Stockholm, October 2013
Ulrik Franke, SPIS project manager

Table of contents

1 Introduction

The information society has changed our way of life. We increasingly work, play, shop and socialize using electronic information and communications technology (ICT) in ways not conceivable a mere decade ago. This poses new challenges for social science, but also for private and public decision-makers.

This study was conducted as part of the Swedish Defense Research Agency (FOI) project "National Security in the Information Society" (SPIS). SPIS is an in-house research project, intended to develop methods for studying the interplay between ICT and social and political events, as well as to explore the role and functions of modern ICT in international relations.

One important background for this work is the debate that surfaced in the context of the so-called *Arab spring*. A more thorough discussion can be found in Eriksson et al. [40]. In this study two key observations were made. First, ICT can have a positive effect on mass mobilization, and thus contribute to bringing authoritarian regimes down, though the technology is neither necessary nor sufficient to cause such events. The role of these 'liberation technologies' is further discussed in Gasinska et al. [50].Second, the outside world plays an important role, both when it comes to the international media scene and regarding technology transfer and export restrictions.

For example, the European Union discussed the possibility of a joint position to impose restrictive measures on Syria's telecom sector [28]. More specifically, the measure included a ban on the supply of software for communications interception, thus targeting telecommunications companies. The ban was meant to undermine the al-Assad regime's capacity to locate opposition forces [97]. Proponents of this policy initiative suggested that forceful measures were needed to maximize pressure on the Syrian regime. However, the EU member states turned out to have different understandings of the implications of such a policy. For example, finding itself politically isolated in its view, Sweden argued for the need to continue an engagement with Syria in the area of telecommunications [29]. The argument was that a continued trade-flow in this area would enable the Syrian population to reach the outside world in spite of the regime's propaganda barrier. On the other hand, Sweden was criticized based on the perception that it merely sought to protect Ericsson's business dealings with Syrian companies. In all, the debate illustrates the dilemma of imposing a ban on technologies – and the close connection between policy and research questions.

The aim of this study is to illustrate perspectives and methods for studying the interplay between ICT and social and political events. As such we have aimed for a broad coverage of available scientific and scholarly methods. We have also chosen to accompany this theoretical research perspective with two chapters that

are more practitioner-oriented, covering the areas of ICT sanctions and privacy, respectively.

1.1 Overview of the report

The remainder of the report is structured as follows. Following this introduction, the literature surveyed in the report is briefly introduced. The ensuing five chapters present different perspectives on and methodologies for security studies in the information age. The report concludes with a discussion of challenges and an outlook.

2 Outline of the literature surveyed

There are many ways to study the interplay between ICT and social and political events. The literature abounds with examples in the entire spectrum from technical to social science. This report is intended to be a showcase of that abundance.

The difficulty can be traced to the *interplay* between technology and society. Carlsen et al. explain that a society and a technological artifact at a given time interact with each other so that both are different at a later time [21]. But the exact nature of these changes is – of course – unknown. What we do know is that the co-evolutionary paths that society and technology follow need to be investigated together.

There is no definite source for a taxonomy of scientific methods that covers all relevant research on technology, society, and their interplay. Instead, a few different sources and views have served to inspire the structure of this report.

The first natural place to look for relevant literature is *social science*. Here, we follow Hollis [62] – a well-cited introduction to the philosophy of social science – in categorizing work according to two dichotomies: explanation vs. understanding, and holism vs. individualism. This sets a rather large stage, highlighting the wealth of methods available.

The second natural source of literature is that of *technology assessment*. Here we use (part of) the taxonomy proposed by Tran & Dim [114] to categorize relevant work into familiar categories such as impact analysis, scenario analysis and risk assessment.

A third interesting view is that of *intelligence analysis*, because intelligence is precisely in the business of assessing the interplay of different and uncertain evidence and produce policy-relevant assessments. We use (part of) the taxonomy of Agrell [3], to place contributions into the two categories patterns and analogies and defining factors.

Fourth, a natural extension of the intelligence analysis support to decision-making is to consider practical consequences of such decisions in the form of *ICT sanctions* and other measures that states can implement to affect other states. These *practical* foreign- and defense policy methods in the area of ICT complement the picture given by the three preceding theoretical perspectives.

Fifth, it is impossible to understand the modern information society without an account of *privacy*, its changing face and its implications. This final perspective differs from the previous ones by including a *normative* strand, stemming from legal studies and philosophy.

The actual literature studied is, of course, not exhaustive. The aim has been to show the wealth of methods – breadth first, rather than to cover everything written on particular subjects – depth first. Following the overall structure of the SPIS research project, a few areas have been especially prioritized, in particular the geographical areas of the Middle East and Northern Africa, China, and Russia, the topical areas of sanctions, integrity and privacy, and the methodological area of simulation models.

It should be stressed that the different perspectives sometimes intersect. A single piece of research might well fit into both the philosophy of social science taxonomy and the intelligence studies taxonomy at the same time. In this sense, the ensuing chapters offer more of a narrative binding various strands of research together, than a definite taxonomy in its own right.

3 The social science perspective

Hollis divides social science according to two dichotomies: explanation vs. understanding, and holism vs. individualism [62]. This gives rise to the following matrix, used as a visual cue throughout his book:

	Explanation	**Understanding**
Holism	Systems	'Games'
Individualism	Agents	Actors

Holistic explanation accounts for action based on social structure. Hollis' token example is Karl Marx' Preface to *A Contribution to the Critique of Political Economy*, where it is argued that material productive forces control not only the actions of individuals, but also leads them to have false beliefs about the reasons for their actions. The proper way to study society, according to this view, is to seek out and map the large-scale laws governing its movement, much like the Newtonian way of studying the solar system.

Various schools in fields of war, peace, and security studies have placed great emphasis on structural conditions to explain both events in the international system at large and particular conflicts. Not least during the Cold War, states and their security and defense 'behavior' have been explained in the literature on basis of structural conditions. In this vein, putting pressure on a leader often meant declaring war or isolating an entire country (embargo, economic and technological warfare, etc.) [75].

Individualist explanation, on the other hand, accounts for social structure in terms of individual action. Hollis' token example is John Stuart Mill's *A System of Logic*, where it is argued that the laws of phenomena in society are nothing but the laws of individual human nature, suitably combined. However, even though individual action then becomes the focus of investigation, the goal is still remarkably Newtonian. Indeed Hollis' category of *explanation* is committed to a single philosophy of science, the same for natural and social science alike.

In peace, security and intelligence studies, this is reflected by the strong attention to agency. Unlike states, previous the unit in focus economic warfare, economic sanctions against decision makers need to consider that such targets can reason, respond and react, thereby creating a complex web of behavior and attitudes (as opposed to states that responded through one official policy held view) . Hence, to change a security situation (e.g. armed conflict or crisis) engaging agents become central. For example, in the case of the civil war in Syria this would mean putting pressure on al-Assad's regime by putting pressure on government

ministers, regime associates and family members. In fact this sometimes even more easily done than engaging policies that are meant to change systems as it does not risk complicating inter-state relations. For example, it does not have consequence for the international system, nor does it give reason for a government to turn its entire society against the sending state. This was the case for Iraq and the comprehensive sanctions regime put in place by the United Nations Security Council.

The *understanding* categories challenge this view, in the spirit of interpretative or hermeneutic social science. Put as a slogan, it maintains that society needs to be understood from within, not explained from without. Whereas Marx and Mill seek the *causes* of actions, the social scientist in the understanding tradition seeks the *meaning* of action, as perceived from the inside, by those who perform it. Ludwig Wittgenstein's notion of 'game' is useful here: moves within games are only meaningful to analyze within the confines of that game, be it moves in chess or utterances in a language. In sociology, this mode of investigation is closely associated with Max Weber, who made the distinction between *verstehen* (to understand) and *erklären* (to explain), where the former term is now commonly used in English to denote interpretive social science. Holistic understanding is the form of investigations that focuses on social roles and positions, where the game in a manner of speaking absorbs the players. Individualist understanding reverses the direction of understanding, based on the conviction that the meaning sought is individualist at its core. Hollis' token example is Jon Elster, who maintains that "there are no societies, only individuals who interact with one another" (cited in [62], p. 19).

In international relations, *realism* (focusing on states, and their national interest to survive in an anarchic world order) and *liberalism* (focusing on international institutions, non-state actors and interdependence) broadly belongs to Hollis' explanation category. Since the late 1980s, however, a (social) *constructivism* that broadly belongs to Hollis' understanding category has also gained a lot of influence. Notable areas of constructivist research related to ICT include the framing of technology issues as matters of security and the symbolic politics of defacing websites [38].

Of course, these categories are not really clear-cut. Many social science studies fall somewhere in between. This will also be evident in the categorizations below. However, the aim is to show the breadth of available approaches rather than offer a definite classification of methods.

3.1 Holistic explanation

Best & Keegan [13] offer an example of a systems level explanation, in their analysis of the relationship between the Internet and democracy using the four regulatory forces first introduced by Lessig [78]. The Internet is affected by law,

markets, social norms, and architecture ("code"), each of which has its own means of sanction, and hence a particular effect on it. Individuals do not figure in this explanatory system, either as components that set things in motion, or as being moved. The explanatory nature of the analysis is further emphasized by the authors' sketch of how to operationalize it with statistics.

Hussain & Howard investigate the role of information technology for democratization, propelled by the example of the Arab spring [63]. In the analysis, they construct a formal model, where factors such as digital connectivity, levels of unemployment, and censorship sophistication feature. In the end they conclude that information infrastructure and in particular cell phones are important factors for explaining regime fragility and social movement success.

Investigating China, Zhao explains how the practice of censorship has changed depending on the overall economic model of society [119]. Before the reforms of 1978, both print and broadcast media served merely as a 'party organ'; today the media needs to strike a balance between being a party mouthpiece and turning a profit. As explored by Zhao, this impacts the journalistic practices of Chinese Internet news media today. Similarly, Herold points out that what sets China apart from many other countries today is that the state owns Internet infrastructures; Internet service providers are only allowed to lease bandwidth. This structural factor makes everything that happens on the Chinese Internet dependent of the explicit or implicit approval of the ruling Communist party [60].

Betz & Stevens, in their exploration of the meaning of 'cyber power', [14] (p. 45 ff.) offer some good examples of holistic explanation. *Institutional* cyber power, they explain, is wielded in organizations such as the Internet Corporation for Assigned Names and Numbers (ICANN), the International Telecommunication Union (ITU) or the Shanghai Cooperation Organization (SCO), and to properly understand the behavior of states in these forums, it is important to realize that an institution can work so that it "guides, steers, and constrains the actions (or non-actions) and conditions of existence of others" ([10] cited in [14] p. 47). *Structural* cyber power is another example, where the contrast with individualist explanation is stressed by the authors, as they "are more concerned with how cyberspace helps determine these structural positions than with how the resulting actors shape cyberspace per se". The investigation of structural power leads Betz & Stevens to consider the transition from industrial to post-industrial economies and the effects of the network society on the positions of capital and labor. However, as we shall see below, other facets of cyber power belong not to explanation but rather to understanding.

A theoretically intermediate form of explanation is the *flock theory*; a theory of emergent self-organization. Though it does speak of the behavior of individuals, its primary object of study is the 'flock', i.e. the behavior of an emergent

community larger than the individual parts. Rosen et al. employ it to study two political protests: against the FARC guerilla and the South Korean government respectively [107]. Based on these observations, they conclude that the Internet plays an important role in the decentralized coordination observed in both political movements.

3.2 Individualist explanation

Farrell takes an individualist approach in his article that map's out Internet's consequences for politics [41]. In his study, Farrell identifies three interesting causal mechanisms where the advent of the Internet gives rise to social phenomena. First, he considers transaction costs of collective action, where agents will find it easier or cheaper to communicate using online tools. This makes is easier to e.g. coordinate demonstrations. Second, communication on the Internet makes it easier to find and interact with others who share particular interests. On the macro level, this can result in *sorting effects*, where people cluster with like-minded others, affecting the political landscape. Third, individuals have incentives to conceal their preferences in many social settings (i.e. "preference falsification"). For example, in an authoritarian state, the regime may be widely loathed, yet everyone disguise its real view for everyone else out for fear of the consequences of revealing their true political preferences. If, in such a society, a new arena arises, e.g. on the Internet, where preferences can be revealed without dire consequences, this can quickly change the general view on the popular support for the government. Each of these mechanisms explains macro phenomena by recourse to the micro level of individual behavior and choice.

An interesting example of an individualist explanatory model applied to the Chinese censorship of social media is Lagerkvist's use of the principal-agent model to analyze the relationship between state and companies [71]. The principal-agent model explains the difficulty of the *principal* in motivating the *agent* to act in the principal's best interest, rather than the agent's own. The model is widely used to describe the relations between principals such as voters or shareholders and agents such as politicians or CEOs, often with a game-theoretic formal representation. In Lagerkvist's analysis, the politicians of the state (principal) have outsourced large parts of online censorship to private companies (agents), thus finding themselves in a principal-agent dilemma that has only been solved temporarily. However, the categorization of Lagerkvist's use of this inherently individualist model is not unambiguous: both the state and the companies are collective entities with a streak of holistic explanation.

Of course, individualist explanation models often render themselves well to be formalized mathematically and investigated using computer-based (agent) simulation methods. In the most interesting models, simple individual rules lead

to complex and unexpected behavior. A good example is Casilli & Tubaro, who investigate the effect of Internet censorship on violence [22], inspired by the 2011 riots in the UK. They re-use an agent based model of civil violence following Epstein [36], where agents can turn violent depending on personal dissatisfaction in combination with the social surroundings. By examining the effects of varying the range of agent perception ('vision') in the model, they construct scenarios corresponding to more or less online censorship, and conclude that less censorship, while certainly allowing for outbursts of violence, also allows the levels of violence to dissipate very quickly. However, the stronger the censorship, the higher the levels of endemic violence over time.

Tan et al. use an agent based simulation model to investigate the opinion dynamics of 'Internet events' in China [112]. Using a five-party agent model (two opposing parties, the media, the government, and the netizen community), complete with actions and interaction rules, they model (i) the 2010 milk powder formula scandal and (ii) the 360 v. QQ competition stand-off in 2010, when compatibility issues between the instant messaging service *Tencent QQ* and the antivirus software *360 Safeguard* were used as a means to stifle competition. The simulations show a decent fit to measurements of the real opinion dynamics during the events. It is interesting to note that while agent-based simulation models are a tool typical of individualist explanation, using agents such as 'the netizen community' places this piece of research quite close to holistic explanation.

Ackland et al. present an agent simulation model that captures the sorting effects introduced by Farrell above [2]. The model describes the linking behavior of political blogs, and explains how observed differences in linking behavior between different political groups can be generated by a simulation model that accounts for the underlying population distribution of political preferences.

3.3 Holistic understanding

When shifting from *causes* to *meaning* of action, discourses and interpretations become important. Lagerkvist & Sundqvist offer an interesting example of how the meaning of criticism online is not always what it seems [72]. The authors find that the microblog tweets on Sina Weibo often criticize certain activities of the Party, but never challenge its hold on power. They coin the term *loyal dissent* to describe this feature, and conclude that microblogging, despite its role as a carrier of criticism, so far cannot be considered a catalyst for democratization.

Another good example of holistic understanding is the analysis of how unified meaning can emerge in a competitive media landscape by Ray [102]. He argues that this shared meaning of reality was a likely prerequisite for the coordinated action during the Arab spring revolutions. However, there is also an individualist

strand in the argument, insofar as this oppositional narrative is said to have gained strength from its roots in "the people's 'real-world' political practices".

Revisiting Betz & Stevens in their exploration of the meaning of 'cyber power', we also find an example of holistic understanding [14]. *Productive* cyber power is a category that readily fits within the framework of hermeneutic social science, as such power is constituted by the ability to discursively construct cyberspace social subjects. Betz & Stevens describe the re-construction of 'hackers' as threats to national security as a case in point.

The re-construction of the hacker concept is, however, just the tip of an iceberg. Eriksson has studied the swift conceptualization of IT as a security problem in Sweden at the turn of the century [37]. He concludes that a confluence of conditions paved the way for this securitization: (i) the end of the Cold War, (ii the breakthrough of IT in society, (iii) the existing connection between military affairs, information and technology, (iv) the ability of the military-bureaucratic establishment to adapt to new circumstances, (v) the lack of oppositions, and (vi) the boost provided by the looming threat of a Y2K bug that would wreak havoc with computers on January 1, 2000. Whereas Eriksson's analysis is strictly constructivist, Nicander gives a broader account of much the same subject, supplementing real and perceived threats with other factors such as constitutional structure, the character of the state bureaucracy and top-down policy coordination [93]. A similar constructivist analysis of US cyber-threat debate is given by Dunn Cavelty, who focuses in particular on how cyber-terror is being framed [23].

The meaning of the public sphere is investigated by Nanabhay & Farmanfarmaian, who stress how activists can renegotiate the meaning and visibility of the public sphere through high-profile protests [91]. In the case of the Arab spring, they explain how social media triggered mainstream media, creating what they dub an *amplified public sphere*. Benmamoun et al. approach the same revolutions through a similar theoretical construct, the *virtual public sphere*, to investigate the role of multinational companies such as Facebook and Twitter [12]. Zahra Sands explores how the online space of the Internet fosters changes in Muslim identity [109]. She concludes that there is a global shift ongoing from a print culture to a 'multimodal' one, and that the political discourse on the Internet is different from earlier oral and written traditions of communication. All of these investigations represent a research strand that in a sense descends from the hermeneutic *Öffentlichkeit* (public sphere) concept introduced by Jürgen Habermas.

An interesting attempt to analyze the issue of 'cyber power' from the perspective of a decision-maker is Fuerth's essay on how it looks from the perspective of the US president [49]. He primarily argues that cyber power is a 'wicked problem', one that is complex, non-linear, and for which no easy solutions exist. (This description would also fit as a description of the whole field we attempt to

capture in this report.) Arguing that a panoramic view of the issue ultimately must exist "in the mind and the office of the President", he expresses the tension between holistic and individualist understanding: ought the president to be understood foremost in terms of his role as president (the office) or as the individual actor? In the end, however, Fuerth's emphasis on the policy making process, and the organization of the White House staff, places his analysis in the holistic understanding category.

3.4 Individualist understanding

Gleave et al. offer an interesting conceptual and operational definition of the 'social role' concept online [55]. The authors construe the concept as a combination of social psychological, social structural and behavioral attributes. They also operationalize online social roles so that they can be measured and analyzed. The bottom-up direction of the process is highlighted as the authors discuss the understanding to be gained by introducing the concept of 'social role ecologies', where e.g. the interactions between 'Question People' and 'Answer People' on Usenet can be examined.

Marolt struggles with how to best understand Chinese 'grassroots agency' on the Internet, and its consequences for the Internet control exercised by the state and communist party [88]. Based on a discussion about the complexities of censorship and self-censorship, irony and humor, and the infiltration of paid pro-party web commentators, he concludes that European concepts such as 'civil society' or the 'public sphere' of Habermas are not readily applicable to the Chinese context, because "observations of Chinese netizens show that they do *not* define themselves in opposition to China's party-state" (emphasis in original), but rather avoid issues such as legitimacy, control and censorship. This leads Marolt to embrace a research method based on individualist understanding, given that the "Chinese Internet is a highly complex public space inhibited by myriad individuals and groups, permeated by subspaces". Marolt is inspired by Keane, who also criticizes the applicability of Habermas to China [67]. Keane instead proposes an understanding based on the difference between 'big' (official, party, mass-movement) and 'small' (influence, personal ties, behind the scenes) politics. Thus, even if 'big' politics makes the official rules, still "[t]he players construct the games of social life", as Hollis puts it.

As a final note on individualist understanding, it is interesting to observe Lonkila's call for moving even *below* the individual as the unit of understanding [83]. Lonkila perceives a need for future research to study not only the *macro* (holistic) and *micro* (individual) levels, but also a *nano* level, e.g. specific actions such as 'liking' something on a social network such as Facebook.

4 The technology assessment perspective

Tran & Daim, in their thorough review of forty years of technology assessment, broadly differentiate between two categories of methods: those for public decision-making and those for business and non-governmental use [114]. In the following, we examine the use the methods for public decision-making to shed light on security studies in the information age.

4.1 Structural modeling and system dynamics

Structural (equation) modeling and system dynamics are mathematically based models, where causal relations between variables are modeled with equations. System dynamics is a powerful way of simulating the behavior of complex systems, with stocks and flows of various quantities.

Lang & De Sterck is a good example of a system dynamics analysis of the Arab spring [73]. The basic component of the model is a differential equation that represents the fraction of protesters or revolutionaries in a population. By letting the growth of the number of revolutionaries depend on functions reflecting *visibility* and *enthusiasm*, the model goes some way to show how the Internet and social media, but also TV and cell phones can influence the pace of a revolution. In the article, Lang & De Sterck offer case studies of Tunisia, Egypt, Iran, China, and Somalia, showing that the model – with suitable parameters and, sometimes, initial shocks, can be made to fit each of these cases. A strength of the simple model used is that its parameters space can be straightforwardly characterized, e.g. depending on the dynamic stability of the corresponding model solutions. It should be noted that the authors argue that the model – despite its quantitative flavor – is primarily a valuable tool for qualitative understanding of the complex revolutionary process.

4.2 Impact analysis

Impact analysis includes a broad category of quantitative, (e.g. decision-trees with probabilities and utilities), qualitative (e.g. the Delphi method) and cross-disciplinary methods.

Kalathil & Boas offer an example of a broadly qualitative impact analysis, aiming to uncover “the impact of the Internet on authoritarian rule” [66]. To do so, they study four categories of Internet use; (i) civil society, (ii) politics and the state, (iii) the economy, and (iv) the international sphere, along with state Internet policy and governance structure. To account for different national

contexts, they also add in a number of basic political, social and economic factors. The analysis then proceeds in an informal narrative fashion, where the eight countries studied are treated one after another, followed by a conclusion that highlights the complex nature of the subject area. The resulting policy implications are primarily warnings against oversimplifications.

A slightly more formal method is the kind of qualitative cross-impact analysis, employed by Jensen in an effort to analyze the impact of four global trends on the problem of terrorism [65]. The four trends – pertaining to Internet use, ethnic and religious sensibilities, economic inequality and US status as a superpower – are systematically examined in a cross-impact analysis matrix to see how they interact. The main intent of the exercise, according to the author, is to stimulate discussion.

4.3 Scenario analysis

One ambitious scenario analysis – situated somewhere in between private sector market analysis and public sector policy analysis – is the Future of the Internet scenario published by Gartner, a consultancy, in 2012 [98]. Three forces are identified as shaping the future of the Internet: a desire for freedom (on the part of online communities and 'netizens'), a drive for profit on the part of companies), and a demand for control (on the part of governments). Based on these driving forces, three 'extreme' scenarios are generated, viz. "the Global Community", "Pay as You Surf", and "Big Brother is Watching". Furthermore, three 'compromise' scenarios, where two driving forces beat the third are also described: "Pay if You Want", "the Egalitarian Web", and "Power and Profit". The time perspective adopted is ten years, i.e. the scenarios aim to describe the situation in 2022. While the scenarios are not intended to predict any single version of the future, they do aim to identify leading indicators that allow decision-makers to identify the relative progression of the forces at play.

A broader scenario, which does not only concern the development of the Internet, is the Global Trends 2030 report, published by the US National Intelligence Council [92]. In this publication, four 'megatrends' are identified as driving change in the world until 2030: (i) individual empowerment, (ii) diffusion of power, (iii) demographic patterns constituting an "arc of instability" and (iv) a food, water, energy nexus. These are underpinned by statistically quantifiable phenomena such growth of a middle class, technology diffusion, shift of economic power, aging, urbanization, food and water consumption and energy usage. Information and communication technology, in these scenarios, instead take on the role of a potential 'game-changer', i.e. something that could change the direction of the megatrends. More specifically, three ICT developments are identified as having a potentially upsetting impact: (i) storage and computational capabilities regarding 'big data', (ii) social networking technologies, and (iii) the

rise of ‘smart cities’, where ICT enables new urban infrastructures. In the end of the report, four alternative worlds are depicted, and the potential impact of the ICT game changers in each of these is discussed.

4.4 Risk assessment

Risk assessments use a structured method to address risks associated with a certain activity or threat. Typically, risk is construed as a combination of the *probability* that a threat will materialize and *consequences*, should it do so. Risk assessments can also include planning for *proactive* or *reactive* countermeasures.

Lewis offers an example of a risk analysis, albeit informal, of ‘cyber terrorism’ and ‘cyber war’ [79]. He concludes that cyber arms are less potent weapons than previously thought, and conversely that nations are more robust than early analysts believed.

A far more ambitions and extensive risk analysis is the Global Risks Report issued in early 2013 by the World Economic Forum [35]. The report reflects the collated judgments of over 1,000 experts on (i) the likelihoods and (ii) impacts of 50 global risks. These risks are interconnected into a network that reflects their potential interactions, and out of this network three ‘risk cases’, each representing an “interesting constellation of global risks”, are more thoroughly explored. Though reminiscent of scenario analysis, the authors stress that their risk assessment is methodologically different in that it does not “attempt to develop a full range of all possible outcomes.” The *Digital Wildfires in a Hyperconnected World* risk case elaborates on how the global information infrastructure could be used for massive digital misinformation, accidental or willful. The authors suggest that their risk analysis could be used as input into more refined scenarios built by other stakeholders to suit their particular domains of interest.

4.5 Decision analysis

Decision analysis is similar to scenario analysis in that future developments are analyzed, and to risk assessments in that probabilities and consequences are often employed. The central difference, however, is the role played by a decision-maker, who can affect the outcomes. Influence diagrams and decision trees are common formal tools.

Boas presents a qualitative decision analysis of the interplay between US policy against Cuba and Cuban domestic Internet policy [15]. The analysis indicates that the ‘dictator’s dilemma’ – “allow Internet and risk being overthrown, or forbid it and risk economic stagnation” is too simplified. The Cuban experience suggests that authoritarian regimes have more options at hand.

A more formal decision analysis of cyber deterrence and cyber war is given by Libicki, who analyzes the costs and benefits for states of retaliating or not retaliating against cyber-attacks [81] (Appendix B). The analysis proceeds from simple decision trees to an example calculus with probabilities and utilities. Though it is difficult to find conclusive evidence, Libicki concludes that it is far from obvious that an explicit deterrence policy is preferable. Indeed, he echoes this analysis in a more recent *Foreign Affairs* article, arguing that retaliation risks unnecessary escalation and that the best way for the US to prevent cyber war is to adopt “technical and political measures to discourage cyber-attacks before they happen” [82].

5 The intelligence analysis perspective

Key areas of the intelligence studies field attempt to assess the interplay of different and uncertain evidence and produce policy-relevant assessments. For example, Agrell lists eight methods of intelligence work [3], some of which are relevant in this context.

5.1 Patterns and analogies

Introducing patterns and analogies, Agrell stresses the importance of previous information [3] (p. 79). Background information, he argues, enables us to quickly discern anomalies from normality, even when these anomalies are small. But finding patterns in complex chains of events can require huge amounts of information. Similarly, knowledge of the past lets us see analogies between past and present events, aiding our understanding. However, Agrell also reminds us of the risks involved: it is tempting to find patterns that are not really there, by mistake or by adversarial deception.

One area where patterns are important is the spread of information in social media. In the wake of reports on use of YouTube- [45], Facebook and Twitter [103] [99] for propaganda, there has been an increasing interest in researching the patterns of such communications. Lee et al. describe social media as a "prime target for strategic influence" and investigate methods for finding campaigns in social media [76]. The methodology uses the similarity of message contents – their 'talking points' – to link messages to each other in message graphs, corresponding to campaigns. Ratkiewicz et al. have investigated the prospects of identifying so-called 'astroturfing' campaigns on the Internet [100] [101], i.e. influence activities that give the false impression that a large grass-root movement is behind a certain opinion. They differ from Lee et al. by adopting a methodology that is based not on contents of messages, but on their pattern of diffusion. Lee et al. report a 90 % accuracy in the ability of their algorithm to tell legitimate from astroturf memes, but also stress that this is probably due to the fact that the astroturfing identified are actually failed attempts. Once the memes spread, they conclude, they become virtually indistinguishable from the normal patterns.

Historical analogies are often used as a means to understand the effects of new technology, by reference to known previous cases. Thus, Anderson argues that contents rather than means of communications are the key to understanding upheavals such as the revolution in Egypt in 2011 [7]. Facebook, she argues, simply played the same role played by print newspapers and the telegraph in 1919, when US president Woodrow Wilson's famous Fourteen Points speech encouraged national liberation movements around the globe. Similarly, Dartnell draws on historical analogy to point out that the enthusiasm for the democracy-

making potential of the Internet in the wake of the Arab spring parallels the enthusiasm for the newspaper in post-revolutionary France in 1789 [31]. Diamond agrees and observes that the printing press not only played an important role for the reformation, the renaissance, and the scientific revolution, but also helped create the censorship of the modern state [34].

de La Chapelle, analyzing the emergence of the multi-stakeholder governance system that has emerged on the international arena with regard to global Internet governance, makes an analogy between Thomas Kuhn's scientific paradigm shifts, and the perceived political paradigm shift fostered by the Internet [32]. Based on this analogy, he goes on to analyze why Internet-related issues are difficult to address within the UN system, how this led to the multi-stakeholder governance concept, and why this new concept might transform the entire international system.

5.2 Defining factors

Defining factors (Swedish: *gränssättande faktorer*), as explained by Agrell, are bottle-necks (limitations) and thresholds that restrict the options available to an actor [3] (p. 93). For example, he argues, a Soviet invasion of Sweden during the Cold war was not feasible with air-transportation only. Given the assumption that harbors would be blocked and defended, the initial attack must be made by amphibious assault somewhere along the coastline. Thus, the few select amphibious vessels capable of carrying out such activities became the defining factor for an invasion, and their whereabouts and behavior became one of the most important early warning indicators monitored by Swedish intelligence. Other examples of limiting factors might include logistics, infrastructure, telecommunications etc.

Perhaps the most obvious case of reasoning by defining factors in the realm of national security in the information society was demonstrated not in scholarly research, but by President Mubarak in Egypt in his decision to shut down the country's Internet access on the eve of his ousting. This is a logical course of action for a dictator who believes in the *digital evangelists* (cf. Comunello & Anzera [25]) who emphasize the revolutionary role of social media. Regardless of whether such a belief is justified, the mere belief in it thus spawns consequences. A description and evaluation of the role of social media in the Arab spring is given by Eriksson et al. [40], who conclude that ICT in some cases was a force multiplier for the opposition, but did not cause the uprisings. Some scholars go even further. Hassanpour for example argues that Mubarak's decision to "pull the plug" on the Internet actually provided an unintended rallying call to the opposition and thus accelerated the downfall of the regime [56].

The flip side of censorship as defining factor is the argument, often made, that the Internet by its very architecture limits the effects of censorship. Thus Zhao argues that the Chinese practice to enroll Internet service providers to filter undesirable contents or refuse certain people access to the Internet "may prove to be fruitless and futile" [119]. Unsurprisingly, much research has been devoted to Internet circumvention of censorship: from Dartnell's study of Peru in the 90-ies [31], to Ahmad et al. [4] and Abbott [1] who study Malaysia and Singapore in the 00-ies, to Alqudsi-Ghabra [5] and numerous others who discuss the case of the Arab spring.

What is perceived as defining factors is not always obvious, however. King et al., studying online censorship in China, conclude that the aim of the censors is not so much to silence dissent and criticism, as to suppress all kinds of collective action [69]. The Chinese regime, apparently, considers mobilization rather than motivation to be the crucial defining factor on oppositional activity.

The technology and organization used by online censors sometimes limits its reach. The Chinese microblog censorship system is labor-intense and largely depends on manual screening of contents – though it is clear that systems automatically flag certain contents, the decision to remove it is taken by a censor [69]. This time-lag means that some messages will reach a certain circulation in the mean-time, before removal. A similar factor limiting the effectiveness of online censorship is the limited ability of both humans and computers to see through wordplay, irony and ambiguity. Add to this the common Chinese microblog practice of tweeting using images of text, thereby making it more difficult to detect sensitive words and topics. These limits to the effectiveness of online censorship explain why many scholars have identified *self-censorship* as a cornerstone of Chinese government strategy [80] [86].

Krueger offers an interesting methodological approach, where Internet access is studied as a limiting factor to political participation in the US [70]. Krueger empirically explores what political participation would look like if equal Internet access were achieved, as near ubiquitous connectivity is indeed now bringing about. He concludes that if the limiting factor of unequal access were to be removed, the Internet could bring new types of individuals into the political process, rather than just replicate or reinforce existing patterns of participatory inequality.

Indeed, there is a large strain of research dedicated to understanding whether the new availability of information through the Internet will change the established patterns of political participation. Unfortunately, so far there is no scholarly consensus on this issue. A meta-analysis from 2009 (based on 38 separate studies) on the one hand provides strong evidence that the Internet does not have a negative effect on engagement, but at the same time fails to establish that Internet use has any substantial impact at all on engagement [17]. Interestingly, though, the same meta-analysis also finds that the effects of Internet use on

political engagement seem to increase non-monotonically over time, suggesting that even if the Internet was not a defining factor in the past, it might still become so in the future.

One formerly defining factor, that has now lost much of its power, is physical distance. Betz & Stevens observe that cyberspace reduces the distance between actors to virtually zero for some kinds of interaction, bringing a large number of weak and formerly distant players onto the playing field. Hence, they conclude that the "main effect of cyberspace on the present international order is subversive" [14] (p. 104).

As a final note, it is worth observing that intelligence analysis itself is being transformed by the advent of the information society. Information used to be scarce – now it abounds. Treverton remarked – more than a decade ago – that as collection becomes easier, selection becomes harder. There is a serious risk that policy-makers become overwhelmed in information these days [115].

6 The sanctions perspective

For the past two decades, the international community has increasingly resorted to targeted sanctions. The shift from comprehensive sanctions to targeted sanctions followed the large-scale negative consequences of the Iraq sanctions during the early 1990s [27].

Targeted sanctions are nowadays frequently adopted by actors in the international system to change behavior of specific entities. There are many different methods to the disposal of the international community in this regard (e.g. UN Security Council, the European Union, African Union, etc.). For a review of restrictive measures adopted by the EU, see Giumeilli [54]. For example, sanctions instruments to affect and change the behavior of the other nowadays include measures such as travel bans, assets freeze, ban on equipment to be used for internal repression, commodity ban, etc. [26]. Sanctions can either be imposed for the purpose of having direct or indirect effect. Research in this regard talks about *coercing, constraining and signaling* [53]. During 2014, a large segment of the research community working on sanctions will present a systematic assessment of all ongoing UN sanctions regimes to assess its policy significance.

During the 1990's the research and policy community dealing with sanctions in its new form referred to sanctions as so-called 'intelligent sanctions', later shifting to 'smart sanctions'. Today the proper vocabulary is 'targeted sanctions' or 'restrictive measures'. One of the earlier academic definitions of targeted sanctions has been provided by Cortright and Lopez who defined it as a policy "… that imposes coercive pressures on specific individuals and entities and that restricts selective products or activities, while minimizing unintended economic and social consequences for vulnerable populations and innocent bystanders." [20] This definition focuses both on individual decision-makers and on other forms of entities rather than full isolationist policies of entire states and communities. For example, in the case of Syria, the international community decided to prohibit a trade with regime by imposing a number of sectorial sanctions against regime members, including ICT sanctions, instead of state in its entire.

Thus the rationale of targeted sanctions is to single out different sorts of targets for different purposes and effects. Moreover, it is intended to be a policy that avoids causing unintended consequences that can come as a result of broad based sanctions.

Targets are usually considered to be entities of a ruling regime, members of a terrorist group, etc. Targets can also be judicial entities such as companies (e.g. shelf-companies and organizations act as legitimate actors for other subversive activities) or non-violent organizations in their capacity of supporting a target.

For example, telecom companies could be subject to sanctions should they sponsor an authoritarian regime. Thus, in a number of situations, states and collective security bodies like the United Nations, the European Union, the African Union, the League of Arab States, the United States, etc. impose lists of specially designated entities of this kind to be targeted with restrictive measures. Typically, targeted sanctions are imposed for the purpose of holding accountable entities for specific crimes. For example, listing of entities with assets freeze or a travel ban can follow as a result of being assigned as causing great harm against civilians (genocide, war crime, etc.). Sanctions lists can many times also work as general "wanted lists" for a variety of purposes (terrorism, drug trade, smuggling, money laundering, etc.). Thus, by singling out decision-makers, armed groups, and the like, actors such as the UN aim to hold particular entities responsible for their actions rather than assigning guilt on collective groups (such as entire states or communities).

A starting point for having sanctions effective is to have good understanding of target. Bearing in mind the distinction between holistic and individualist understanding outlined in chapter 3, the challenge for any decision-maker that seeks to change or modify the behavior of an agent, is whether efforts should be concentrated on structures, agents or a combination of both to achieve maximum influence on the intended policy. (For a further discussion on methods and operationalization in this realm, see Eriksson [39]).

Noteworthy however is that any form of targeted sanctions needs to be understood in the broader strategic framework of the sender. Traditional literature on strategic studies offers a number of theories and methods herein. For example, should the intended policy be deterrence; prevention; pre-emptive deterrence; compulsion; retribution; disapproval; punishment; stigmatization; symbolic actions; (signaling); containment [47] [48] [46] [30] [51] [59] [61] [84] [89] [106] [118]. It is also within any of these broader policy strategies that specific instruments can be-used, such as bans or limitations on telecommunications or Internet. What then do targeted sanctions do?

Though much dependent on the strategic approach that is being considered sanctions measures includes preventing targets from acquiring technologies; withdrawing resources that already with the targets; or destroying technologies that are with the target. At times efforts can also include preventing the target from accessing technologies that are needed to develop or repair infrastructure that is needed to access information. Moreover, targeted sanctions include stopping flows of commodities to targets; to stop financial means necessary for targets to acquire or sustain technologies (e.g. payments and transfer means). Usually these efforts come through the adoption of various filters in the financial system (for example by pressing banks to stop suspicious money transfers to a target state); by inspections regimes (e.g. through control and verification of air

and maritime cargoes destined to a particular country under scrutiny, like Syria and Iran); etc.

Beyond these technical approaches there are a number of closely related strategies that could be embraced for achieving behavioral change. Here one could also think of broader socialization strategies like conditionality, norms compliance, naming-and-shaming. The EU's use of these softer forms of pressure with the goal of inducing change, achieving influence and compliance can be found in the writings of Finnemore & Sikkink [42], Checkel [24], Schimmelfennig, Engert & Knobel [110], and Schimmelfennig & Sedelmeier [111]. Through such an approach, a target is teased with policy carrots than by more forceful sticks. For instance, rather than stopping transfers of telecom technology, the sender would offer an increase in trade should the target modify its behavior. The sender also concentrate more efforts to coopt the targets behavior as opposed to stigmatizing its. In all of these contexts both targets and their supporting networks, affiliates and solicitors, etc.

In the context of 'ICT' tools, ICT sanctions are one of the most recent foreign policy inventions. So far however, is has only been tested in Syria. Thus, there is not that much experience of how well it works and what accomplishments one can achieve by using such approach for behavioral change.

Nonetheless, as with some other policy methods, ICT sanctions decision-makers will have to hurdle some ethical challenges when deciding on its use. For example, imposing ICT sanctions could easily isolate a population even more than was anticipated at the outset. What seems essential is that in order to change behavior of a specific target the sender need to tailor-make a policy design. The sender needs to be in conformity with the political dynamic on ground. While some targets may quickly feel the pain of ICT sanctions, other actors may not feel it at all. The literature has also covered this ethical issue. Essentially the main finding in this context seems to be that targeted sanctions work best when they operate in tandem with an opposition on the ground. For example, EU's previous strong sanctions regime on Burma/Myanmar was plagued by opposition group's political in-fighting on whether to have sanctions on the military junta or whether to call for political and economic engagement [116].

Moreover, in some situations the broader population may experience the pain and the 'backside' of this policy, while the elite may go unharmed. Further to this, some situations may prove to be more challenging in terms of implementation. Many conflicts in Africa where targeted sanctions are in use, and where the ICT tool could be applied, may cause more harm for civilians than other. While it could be easy for the elite to circumvent ICT sanctions, the broader population could more easily suffer the consequences as a result of lack of resources and their dependency of having ICT access [50].

Similarly, there are also political contexts where ICT sanctions have the potential to work better or worse. Imposing ICT sanctions against a regime involved in a civil war may be easier than imposing ICT sanctions against a specific group in a particular geographic location of a country engulfed in a civil war (e.g. against a rebel group in the Democratic Republic of Congo, against a terrorist cell in the Sahara.).

Another challenge in this context is the role of propaganda. In several sanctions regimes where the sender seeks to challenge the behavior of authoritarian regimes free speech may be curtailed. For example, governments may be in control of media. In such kinds of context restricting access to Internet and telecommunications may cause problems for the population suffering under such regimes.

7 The privacy perspective

The advent of and widescale adoption of social media has created much discussion regarding privacy. In many instances the case made is that privacy of the individual must be weighed against security of the population as a whole, and that the latter takes priority. However, the right to privacy is enshrined in many legislative documents, including the Charter of Fundamental Rights of the European Union, specifically in the second title. Many nations also include similar rights in national legislation. Privacy is a term which contains many nuances and possible interpretations. While these may be sufficient for normal discussion it is necessary to have a common definition in order to be able to draft and enforce binding standards, especially in the context of new technology which enables covert monitoring on a scale hitherto unthinkable.

This privacy view differs from the previous views on the subject in that research in this area is not only *descriptive* but also contains a *normative* strand. This holds particularly true for subjects such as *information ethics* (cf. e.g. Floridi [44] or Capurro [20]). Technology research related to privacy, on the other hand, is seldom *explicitly* normative. Rather, certain privacy concepts are just implicitly assumed to be good, and the investigation then proceeds descriptively to investigate whether certain vulnerabilities exist or can be remedied. This is similar to the way medical science implicitly assumes human health to be good, or agronomy implicitly assumes flourishing fields to be good, but then most often proceeds by purely descriptive analysis.

7.1 Taxonomy

Bostwick [12] offers an analysis of the concepts of privacy from a legal point of view, tracing the concept at least as far back as the Fourth Amendment to the United States Constitution (adopted in 1792). However, this serves little purpose unless the actual context is considered. Bostwick's analysis considers a number of past cases, and attempts to draw general conclusions. His thesis is that cases involving privacy can be grouped into one or more of three categories [16]:

- The privacy of repose
- The privacy of sanctuary
- The privacy of intimate decision

Warren & Brandeis summarizes in one phrase the three concepts as "the right to be let alone" [117].

The three categories of privacy proposed by Bostwick are briefly mentioned below. The descriptions given are based on U.S. legislation, but should be broadly applicable in any democracy sharing similar social and cultural values.

The privacy of repose: here there arises a possible conflict with the right to freedom of expression. The latter in principle allows uninvited visits (or other forms of uninvited contact, e.g. by e-mail, post or telephone) by commercial interests intent on selling, or persons conveying a message, e.g. by loudspeaker announcements. It was concluded that the right to privacy of repose outweighed the right to freedom of speech.[1] Here it is relevant to compare the situation today, where it is practically impossible to avoid uninvited advertising in one's private letter box, or uninvited e-post ("spam"). The right to privacy of repose enshrines the right to exclude unwanted contact, information, messages, etc. from the private zone.

The privacy of sanctuary: this encompasses the right to protect intangible assets within the private zone, i.e. to prevent third parties from seeing, hearing or knowing about actions within the private zone. The most common example of this is the right to hold a conversation without being intentionally overheard by e.g. wiretapping. Note that this right to privacy may be set aside if "there are reasonable grounds to suspect that a crime has been or will be committed" and that normally a court order or similar is required to intrude on the private zone.

Here it is relevant to compare the situation today, where many governments (e.g. U.S. National Security Agency, NSA and Government Communications Headquarters, GCHQ, U.K.) and non-government (e.g. Google, Twitter, Facebook, LinkedIn) organizations gather, store and filter information about private communications without benefit of a court order, and not always with contractual consent from the customer/user. This is especially common in social media communications, but also in e.g. "street view" situations. It is arguable that the normal user can reasonably expect that his/her e-mail communication is private and may be read only by the intended recipient, by analogy to conventional letter post.

The privacy of intimate decision: this category was originally conceived to cover the most intimate situations, including e.g. the use of contraceptives and later the widely discussed Roe v. Wade judgment[2] covering a woman's right to terminate her pregnancy. This category was later broadened to include the right to read (and by analogy to watch) any sort of material in the privacy of their own home. We may suppose that the category also includes the right to purchase any particular product or service, subject to this not imposing a disproportionate burden on society as a whole (e.g. the case which upheld a person's right to use marijuana in their home[3]).

[1] Judgment handed down in 397 U.S. 728 (1070) at 736-37
[2] 410 U.S. 113 (1973)
[3] Ravin v. State, 537 P.2d 494 (Alas. 1975).

This latter aspect is especially relevant today when it is widely known, or at least suspected that many organizations (both commercial and governmental) collect and save records of the Internet sites visited from a particular computer where the user is more often than not identified. In many cases this is required for administrative tasks such as billing, but it is know that companies are developing tools for highly personalized profiling. This can be also be considered to come under the right to privacy of sanctuary, a user's private zone extending beyond their immediate neighborhood to also include e.g. websites visited.

It is interesting to note that Islam attaches importance to the fundamental human right to privacy, which is referred to in the Quran: "do not enter any houses except your own unless you are sure of their occupants' consent" (24:27) and "do not spy on one another (49:12) (examples from Hayati [57]), which equate to the privacy of sanctuary and privacy of repose respectively.

We can conclude that the private zone is not necessarily restricted to a particular physical location (the home, office or a car) or to a zone around a person. The zone of privacy can extend over long distances, e.g. a telephone call and by analogy an e-mail message which may pass through several routing stations.

We can also conclude that the concept of personal privacy is not new, and has been established in western and in particular the American justice system for many years. This is not to say that the concepts are universally applicable, and it should be borne in mind that this taxonomy was established when it was impossible to conceive of the surveillance & monitoring techniques widely & cheaply available today.

We now look at those aspects of privacy which arise with the widespread use of social media, with the Internet (and devices accessing the Internet) and with our concerns for security.

7.2 Privacy & culture

Concepts of privacy are of course closely linked with personal and cultural values. While basic ethical concepts seem to be universal (e.g. right versus wrong) it seems intuitively likely that these are mediated by local and/or national culture. For this reason it is relevant to study privacy and ICT in Japan, often cited as not having any privacy at all in the sense commonly used in the western world. If it is the case that there is little or no common ground between western and Japanese concepts of Internet privacy then establishing international ethical policies will be difficult. Mizutani et al. have studied the subject, noting that there is no word in Japanese meaning "privacy" [90]. However, if the subject is considered in terms of *normative* and *descriptive* behavior then it is argued that Japan does indeed share many privacy values with western nations. While descriptive privacy may be quite different in Sweden, with for example stronger

physical barriers separating people, normative practices may be equally strong (or indeed stronger). Japan abounds with (to western eyes) invisible barriers related to religion which may not be crossed lightly. Contrasts exist between British concepts of mixed gender bathing (strictly forbidden) and Japanese baths where mixed bathing is the norm. In contrast, in a Japanese home eating utensils (bowls, chopsticks) are used by one person only, whereas this is not the case in western nations, where many individuals share the same utensils. Privacy, as discussed by Altman, and Palen & Dourish below relates to control of access to the self (as opposed to "the group" or society), not merely to forbid access to those not authorized, but to control access under different circumstances. A good illustration is given by Mizutani et al., citing the well-known Japanese practice of after work drinking. In such circumstances it is not uncommon for the senior colleague to suggest dispensing with the normal "at work" rules of hierarchy, i.e. what is said is "off the record" and not to be repeated or used later. Since Japanese houses are normally small, and rooms may be divided by thin paper screens it is inevitable that conversation will be overheard. There is a strong convention (likely stronger than an equivalent situation in the west) that any information accidently overheard will never be repeated, nor even referred to. These are strong social norms. Hence it is shown that western concepts of privacy do indeed exist and flourish in Japan, although naturally mediated to reflect ways of living.

These concepts can be transferred to Internet privacy. A network manager has easy access to e-mail messages (exactly as in the west), but is bound by social norms not to read the messages. In the west it is likely the same would be achieved by rules and regulations, but the effect is exactly the same. Hence it is argued that Internet privacy policies with shared values are feasible.

Bellman et al. have also studied differences in how Internet users (consumers) in 38 different countries perceive Internet privacy [11]. Several differences were observed relating to how Internet users trust the websites they use, how they regard Internet security (e.g. for financial transactions) and how they fear information may be transferred to a third party and used without their consent. However, it was concluded that the differences were related to e.g. how strong privacy regulation is in the country and general characteristics of the society. For example, users in countries with little Internet privacy regulation (e.g. Greece) are more concerned about security of financial transactions, and fear of unauthorized secondary use of data is greater in highly individualistic countries such as the USA.

7.3 Technical opportunities

Modern ICT is one of the strongest enabling factors contributing to the current situation where privacy of the individual is under threat. The situation is dynamic

and new opportunities for monitoring our activities are developing rapidly. However, technology is not the main driving force. Opinions may vary, but often cited factors include:

- Safety (against accident or crime)
- Security (against antagonistic threat to society and/or organized crime)
- Statistical data (for planning and monitoring society's infrastructures)
- Business (for individual shopping)

All the above require collection and storage of personal data, which is to some extent essential for society to function and for individual citizens to enjoy the benefits of a modern society. The main threat to our privacy is that the individual is often unaware of:

- Which data is collected and when
- What the purpose of the data collection is
- Who is collecting the data
- Who has access to the data
- How the data will be/may be shared
- How the data may be analyzed together with other data
- How long the data may be stored or be available
- How to correct/remove/erase/limit the use of the data
- It is impossible to function in modern society without contributing, voluntarily or involuntarily to data collection

Everyday examples can be found in monetary transactions such as buying food at the grocery store, using a cellphone (especially a smartphone) or simply standing in a public space. The list is not intended to be exhaustive. A problem is that once the data has been collected it is in practice impossible for the individual to retain control of the data. We focus here on the more intrusive and less innocent monitoring activities.

Since technology is an enabling factor, technology can also be a part of the solution. Tools exist for anonymous Internet communication, for example TOR (The Onion Router), a system of software and hardware enabling anonymous communication through the Internet.[4] Briefly, the principle is that a message (e-mail) is sent from a computer to a node which removes the sender's address and

[4] The TOR project is found on https://www.torproject.org/. Accessed October 14, 2013.

forwards the message to another node in the TOR network where the process is repeated. By removing the sender's address and forwarding several times the origin of the message can be effectively hidden, i.e. anonymized. Eventually the message is delivered to the intended recipient. A weakness in the system is that if the message is intercepted between the sender and the first node then the sender is revealed. The hardware in the TOR network is largely contributed by volunteers and therefore dynamic, further improving safety against tracking. TOR is seen as a useful tool in situations where there is a large asymmetry between the participants, for example where a state or other organization with large resources wished to identify the origin of a communication. Of course the TOR system can also be used by criminals for illegal purposes, and there is evidence that this does occur.

Poblete et al. coined the term *website privacy* in their investigation of privacy in search engine logs [96]. The motivating example of their research is the infamous 2006 publication of a large data set of web queries from America Online (AOL) users, where it turned out that the anonymization undertaken before releasing the data set was insufficient. A number of users were readily identifiable, and some even had their identities published along with their queries. Poblete et al. discuss a number of techniques to protect website information, and conduct successful experiments with a technique designed to protect against one conceivable attack against anonymized web query logs.

Brynielsson et al. offer a literature review of the growing field of *privacy preserving data mining*, i.e. data mining methods designed to respect privacy in some sense [18]. Basically there are two main strategies: *Sanitation methods* modify data before publishing, so that overall statistical features are preserved, but individuals cannot be identified. *Distributed secure methods* use cryptographic techniques to compute statistical features without allowing direct access to underlying privacy-sensitive data.

However, anonymous messages can still be intercepted easily and if the contents of the message are in clear text it is likely they will reveal the sender's identity. To avoid this risk the message can be encrypted, using one of a number of commercial or openware/shareware programs. The software PGP (Pretty-Good Privacy) is widely available[5] and often used. Again, PGP and similar encryption software is useful in asymmetric situations, although with sufficient resources it is usually possible to decrypt a message. This is in practice only possible by state-sponsored organizations.

However, anonymization and encryption are rather similar to living in a bunker. The individual has only limited access to the external world and many normal

[5] The PGP openware can be download from: http://www.pgpi.org/. Accessed October 11, 2013.

functions are rendered impossible. Privacy is more than anonymous communication and secret identity. One cannot anonymize an on-line shopping transaction for obvious reasons, so these techniques are not a complete solution to privacy preservation. What is lacking is a system which allows the user to *manage* their privacy, in accordance with Altman's model [6] where the degree of openness or closedness is dynamic and controlled by the individual.

Roberts et al. have empirically investigated the use of circumvention tools, i.e. tools that allow users to establish a proxy connection to otherwise blocked sites [105]. They conclude that (in 2010) no more than 3% of Internet users in countries doing substantial filtering use circumvention tools. A thorough review of tools to circumvent filtering, maintain anonymity and encrypt data is given by Ziccardi [120].

7.3.1 Development trends

Langheinrich proposes a privacy awareness system (pawS) which partially solves this issue [74]. He argues that in an environment pervaded by ubiquitous computing (ubicomp) it is technically feasible to maintain a balance between openness and closedness. Important features include (i) notice, (ii) choice & consent, (iii) proximity and locality, (iv) anonymity & pseudonymity,[6] (v) security and (vi) access & recourse, which address most of the threats to privacy listed above.

The pawS features include a *privacy beacon* which alerts and informs the user about the data collection of the service being used and their data collection policies. The user can use a mobile *privacy assistant* to compare this information with the user's personal *privacy proxy* which is stored in the Internet cloud, which in turn interrogates the various service providers about their *privacy policies*. After comparing the privacy policies with the user's privacy preferences the user's proxy can e.g. decline or deny the use of a tracking service, which is switched off.

In this case the system relies on a combination of social norms, legal deterrence and law enforcement to ensure compliance. There are many systems in society which operate on the same principles (e.g. road traffic management) and which are fairly successful. The pawS does not exist yet although some components have been designed and trialed. These include the user's *privacy proxy* and a *privacy-aware* database.

[6] Pseudonymity is the use of pseudonyms as IDs, thus enabling users to access resources without disclosing their identities [95].

Other approaches to privacy preservation in ubicomp environments include automated surveillance. However, critics such as Macnish argue that it is not necessarily the case that fully automated surveillance is better than the manual alternative from an ethical point of view [87].

Smartphones contain positioning technologies (embedded GPS or base station triangulation) which can identify the location of the device (and hence it's user) at any time the device is switched on (and its location when it was last switched off). There is a considerable commercial driving force for this service [43]. Khoshgorazan & Shahabi suggest a taxonomy related to *anonymity/cloaking*, *transformation* and *private information retrieval.* Cloaking relies on the use of a trusted location anonymizer to hide the user's location and identity. The anonymizer is placed between the user's device and the location server and blurs the exact location of the user. It is concluded that the method cannot guarantee to hide the user's location [68]].

7.3.2 Antagonistic activities

In contrast to the above where we know or assume that monitoring activities are in the main performed by known actors (companies, democratic & non-democratic government organizations, criminals) there are many documented cases where persons working on behalf of non-democratic governments and unscrupulous companies, and criminals have posed as normal users in order to spread biased information. The purpose may be to create or quench public opinion, mislead, entrap, commit crime or to libel and defame a person or organization. The concept of '50-cent bloggers' has been coined and refers to the widespread occurrence of bloggers in China who are reputed to be paid 50 cents per blog post in support of the government's political policies [103]. As shown by for instance Lee et al., there is a large commercial market where requesters use crowdsourcing to task workers with placing likes, tweets, search queries etc. – a practice known as 'crowdturfing' (from crowdsourcing and astroturfing) [77].

7.3.3 Censoring activities

It is well know that many nations regularly monitor social media with the stated intention of suppressing dissident thought and restricting freedom of speech and indirectly freedom of association. China, Russia, Egypt, Libya are some well know examples.

How this is done technically varies greatly in the degree of sophistication. China for example can be regarded as relatively unsophisticated, frequently blocking access to websites and servers considered undesirable by the state. Egypt has resorted to the rather brutal method of simply switching off the Internet, limiting (but not entirely preventing) both international and domestic communication.

Russia is thought to employ more sophisticated measures, where false information is published, in some cases with the intention of trapping dissidents.

Much is known about organized Internet censoring, but there is an area which is much less well known, that of self-censoring. If a user of social media knows, or suspects that his/her communication may be intercepted then it is possible that some degree of self-censoring will occur, i.e. the user will refrain from publishing information which may result in reprisals, either officially or unofficially.

7.4 Privacy models

Few published reports have been identified which concern privacy models in the formal sense.

Palen & Dourish [94] have attempted to extend the privacy model of Altman [6] to include the peculiarities introduced by social media and modern information access/information sharing. They consider three aspects not covered by Altman:

- The disclosure boundary: public versus private
- The identity boundary: self versus other
- The temporal boundary: past-present-future

Altman suggests that privacy is a state which is neither static nor rule-based, and that it can be conceptualized as "selective control of access to the self." In other words we (the individual concerned) define boundaries which, depending on the situation allow varying degrees of "openness" or "closedness" (accessibility or inaccessibility). The limitation of Altman's model (as claimed by Pale & Dourish) is that it considers situations where access is mediated by contemporary spatial and temporal dimensions. Hence the relaxations allowed by social media are not considered. By relaxation we mean that the sphere of influence of an individual is not limited to his or her immediate location, but encompasses in principle the entire world (at least those parts of it which are connected by modern communications technology). Temporal limitations are also relaxed in that data can be stored easily, at low cost, in a searchable form more or less indefinitely. Data stored today may still be accessible in 100 years. This is not new, but what is new is the scale of data storage, that it is easily searchable and widely accessible.

Palen & Dourish extend the privacy model of Altman to take into account the disruption of spatial and temporal boundaries caused by modern ICT. Privacy is not simply a matter of limiting access to the self (as in Altman's model); in fact privacy may be enhanced by disclosing information about one's self. Active participation in today's networked world requires some disclosure of information simply to be a part of it, e.g. we enjoy the convenience of purchasing goods via

on-line shopping, which requires disclosing some personal information for the transaction. We enjoy the convenience of rapid communication with friends through Twitter, blogs, Facebook, etc. However, this information which we disclose freely today can be archived and be accessible in new contexts far into the future. This information may also be combined with data from third-party sources (public record databases, address and telephone databases, etc.) and interpreted in ways we did not envisage (and which perhaps did not even exist) when we disclosed the information. The situation becomes even more complex when a third party may make the disclosure, e.g. friends may benevolently post photographs from a recent party which one would not post on one's own initiative. Palen & Dourish refer to this as the disclosure boundary. There is clear potential for problems now and in the future.

The second boundary condition in Palen & Dourish concerns identity, that of self versus others. This may seem self-evident, but in our networked society the situation is complex. We act as individuals, but often also as members of a group or as representatives of a group (e.g. family) or profession. We as individuals are subject to allegiances and affiliations which impose limitations. Inclusiveness and exclusiveness is mediated through the situation and our actions (and those of others). In the everyday world (society) we experience relatively unlimited access to others in our immediate environment, and we can control how our actions appear to and are interpreted by others. In the cyber world our access to those in our environment is not unlimited. Indeed the situation may be reversed, and others may have considerable access to one's self, but not always *vice versa*. Technology mediates the free flow of information, through a website, through a blog or similar social media. Indeed how we are represented in cyberspace may differ significantly from our own perception and the image we wish to project to others. Our image as visible to others may be accidently or deliberately distorted as our identity is affected by the scope and limitations of information others have concerning us. In reality we have very little control of how others see us in the networked world. Simply by being listed on an email distribution list, or by visiting a cookie-enabled website is open to interpretation and control of this interpretation is largely under control of the recipient, although this can easily be manipulated by a third party. Information persistence further complicates the situation.

The temporal boundary is the third relaxation created by social media. Our current actions are based on past actions, and our response to information disclosure are likely to be related to similar situation sin the past. This is not to say that we always react in the same way to a similar situation, conventions evolve with time. However, the ability to distribute information widely may also be seen as a way to influence future events, knowing that information persistence is much more likely today than previously. Hence the temporal boundary has been expanded, although the new boundaries are rather vague and largely uncontrolled at the present.

7.5 Summary

Internet privacy is in its infancy. Regulation is incomplete and inconsistent, and varies widely throughout the world. As is normal, regulation and standards lag behind technological development, and the situation is rendered more difficult as social media and other applications of ICT continue to develop at high speed. As an example where new concerns are likely to arise in the near term (< 5 years) we can consider the smart home, where ubiquitous computing will be employed to monitor energy use and behavioral patterns (for safety of the occupants) and new business models for truly personalized shopping where not only products and services will be tailored to the individual but so will the price.

However, is has been shown that although social media is a modern development, concepts of privacy originally developed and enshrined in legislation in the late 1700's are still applicable, although are subject to mediation by national and international practice.

8 Challenges and outlook

While the wealth of methods explored in the previous chapters show that much research can be and indeed is done, there are also some limitations and challenges.

The most trivial challenge is the wealth of methods themselves. Studying security in the information age can require proficiency in more than one research discipline. Conversely, decision-makers, researchers or indeed anyone in the public would be wise to ponder exactly which questions they want research efforts to answer, not only because different questions require different research methods, but because familiarity with one or a few research methods affects what we find interesting. From this perspective, it is promising to see that combined conferences with contributions from many disciplines are emerging, such as the International Conference on Cyber Conflict (CyCon), running its sixth installment in 2014.

One important limitation is that researchers are in some sense at the mercy of the available material. Sometimes this means that all sources on a particular issue such as Internet usage in China point back to the same official statistics, known to be unreliable. Sometimes, as is often the case in the field of Twitter studies, it is not clear exactly how the samples made available, for free or as a commodity, are put together. This raises important question marks about skewed distributions and potential systematic biases. Sometimes, as in the case of censorship studies, the most knowledgeable parties have an incentive to deliberately keep their data to themselves.

A related issue has to do with research ethics: what data can be made public? Social network research on criminal organizations or opposition movements in authoritarian states are token examples, where the publication of un-anonymized data can entail physical danger to people. This also calls for high standards when anonymizing data which is to be made public.

Language barriers can make the *understanding* methods of Hollis, depending crucially on hermeneutics and properly grasping the meaning of words, difficult to apply from the outside. This is trivially true when a native Swedish or English speaker attempts to decipher Russian or Chinese, but it is also importantly true when a researcher attempts to understand the mindset of an opposition activist, government censor, legislator or netizen-at-large.

When proceeding from merely trying to *understand* someone else to also trying to *affect* that someone's behavior, other challenges surface. In the context of setting up a so-called sanctions regime, seeking to change the behavior of a target

is difficult.[7] There are many different elements that need to be considered. Firstly, targets have a tendency to change behavior and political positions over time, oftentimes reflecting new realities on the ground [39]. Policies adopted by the sender at time X may not be relevant ant time Y. Similarly, the sender's own strategic goal may not be the same over the course of the conflict. For example, the UN Security Council may impose ICT sanctions in a conflict situation to seek a behavioral change. On-ground fighting may change over the years so that sanctions do not play the (intended) role it once did. Sanctions may in fact turn out to work contrary to the original intentions of the UN Security Council. However, a termination of the policy instrument, or even a reversal of the policy intention, may be politically difficult.

Secondly, the sender may have multiple goals. Heads of states of the sending body (e.g. member states of the UN Security Council, the European Union, etc.) may perceive the adoption and subsequent implementation of sanctions as a means to achieve a particular objective. A hypothetical example may illustrate this. For example, a decision by the UNSCR to impose ICT sanctions in the context of the Syrian civil war may be seen by Russia as a way to undermine the armed opposition in its fight against al-Assad. Meanwhile a number of western governments may see ICT sanctions as a way to limit the Syrian regime from functioning in a normal way. Such differing views may cause operational problems for the UN in dealing with the implementation of such a policy. Another challenge regarding multiple goals is that the sender needs to make a trade-off between its sanctions policy and many other ongoing policy instruments in a way that can weaken the main objective. For example, the UN may pursue a human rights agenda, or a freedom of expression agenda, yet UN sanctions may infringe on such principles by targeted sanctions [39]. A third problem is that the imposition of targeted sanctions may work better or worse depending on the situation (i.e. phase) in which the policy is adopted and enforced. For example, the implementation of an ICT sanctions policy may work better as a surprise maneuver at the *outset* of a crisis, rather than in the *midst* of an escalated armed civil war (compare for example with Syria). The sender therefore needs to be aware of how restrictive measures are likely to work in different phases of a conflict [39].

One perspective that is extremely useful for security studies in the information age, but alas works best with hindsight, is the perspective of *unintended consequences*. Whether the concept is associated with Murphy's infamous law [113] or with Nobel laureate F A Hayek [58], technological or social artifacts often turn out to have consequences that were unforeseen and unintended by their

[7] For an overview of all UN Sanctions regimes, see: http://www.un.org/sc/committees/ ; for a similar overview of EU sanctions measures in force see: http://eeas.europa.eu/cfsp/sanctions/index_en.htm

designers. Well-cited studies in the ICT area abound, ranging from unintended consequences of clinical decision support systems in medical settings [9], over the impact of instant messaging technology in the workplace [19] to the inadvertent loss of privacy of Facebook users [33]. On the policy level, many similar cases of unintended consequences can be observed. Mubarak's decision to shut down the Internet did not save him. (Indeed, it might even have accelerated his ousting [56].) US policy since 1992 of deliberately exempting international telecommunications from the embargo on Cuba has not undermined the regime, but rather allowed it to establish and maintain centralized Internet control [15]. Cyber-attacks such as the 2007 attacks on Estonia and the 2012 Stuxnet attack on Iran failed to bring about their (probable) desired policy outcomes [64]. Policies intended to establish 'cyber deterrence', thus decreasing the risk of war, may have the opposite effect [82]. Economic sanctions (possibly including ICT sanctions) can unintentionally contribute to the criminalization of the state, economy, and civil society [8]. Regulations intended to bring about information security instead risk decreasing competition and productivity [52]. Chinese censorship practices, outlawing Internet-borne rumors as 'cyber crimes' [119] punishable by three years in jail [104], themselves contribute to forming a unique media environment that is extremely conducive to rumors [85]. The list goes on. Revisiting Hollis, it can be observed that the concept of unintended consequences is highly useful to understand something afterwards, but less useful to explain or predict it beforehand. Nevertheless, this is a humbling perspective that deserves to be pondered by researchers and policy-makers alike.

One particular challenge that largely sets social science apart from natural and technological science is that theories actually affect the behavior of people. Following the advent of game theory as a paradigm in international relations, it was understood that it matters whether national leaders *believe* that they are engaged in a chicken race or in a prisoner's dilemma when trying to diffuse an international crisis. Similarly, it matters whether diplomats negotiating cyber policy make analogies to the law of the sea, to air traffic control or to the Antarctic treaty (the example is borrowed from Ryan et al. [108]). The choice of how we study security in the information age in this sense matters beyond research, because the choice of research perspectives will color the perceptions of policy-makers, whether intended or not.

9 References

[1] Jason P Abbott. Cacophony or Empowerment? Analysing the Impact of New Information Communication Technologies and New Social Media in Southeast Asia. *Journal of Current Southeast Asian Affairs*, 30(4):3–31, 2012.

[2] Robert Ackland and Jamsheed Shorish. Network formation in the political blogosphere: An application of agent based simulation and e-research tools. *Computational Economics*, 34(4):383–398, 2009.

[3] Wilhelm Agrell. *Essence of Assessment: Methods and Problems of Intelligence Analysis*. Swedish National Defence College, Stockholm, 2012.

[4] Fauziah Ahmad, Chang Peng Kee, Normah Mustaffa, Faridah Ibrahim, Wan Amizah Wan Mahmud, and Dafrizal Dafrizal. Information propagation and the forces of social media in Malaysia. *Asian Social Science*, 8(5):71–76, 2012.

[5] Taghreed Alqudsi-ghabra. Creative use of social media in the revolutions of Tunisia, Egypt & Libya. *International Journal of Interdisciplinary Social Sciences*, 6(6):147–158, 2012.

[6] Irwin Altman. Privacy regulation: culturally universal or culturally specific? *Journal of Social Issues*, 33(3):66–84, 1977.

[7] Lisa Anderson. Demystifying the Arab spring: parsing the differences between Tunisia, Egypt, and Libya. *Foreign Affairs*, 90:2–7, 2011.

[8] Peter Andreas. Criminalizing consequences of sanctions: Embargo busting and its legacy. *International Studies Quarterly*, 49(2):335–360, 2005.

[9] Joan S Ash, Dean F Sittig, Emily M Campbell, Kenneth P Guappone, and Richard H Dykstra. Some unintended consequences of clinical decision support systems. In *AMIA Annual Symposium Proceedings*, volume 2007, page 26. American Medical Informatics Association, 2007.

[10] Michael Barnett and Raymond Duvall. Power in international politics. *International Organization*, 59(1):39–75, 2005.

[11] Steven Bellman, Eric J Johnson, Stephen J Kobrin, and Gerald L Lohse. International differences in information privacy concerns: A global survey of consumers. *The Information Society*, 20(5):313–324, 2004.

[12] Mamoun Benmamoun, Morris Kalliny, and Robert A Cropf. The Arab Spring, MNEs, and virtual public spheres. *Multinational Business Review*, 20(1):26–43, 2012.

[13] Michael L Best and Keegan W Wade. Democratic and anti-democratic regulators of the internet: A framework. *The Information Society*, 23(5):405–411, 2007.

[14] David Betz and Tim Stevens. *Cyberspace and the state: Toward a strategy for cyber-power*. Routledge, for the International Institute for Strategic Studies, 2011.

[15] Taylor C. Boas. The dictator's dilemma? The internet and U.S. policy toward Cuba. *The Washington Quarterly*, 23(3):57–67, 2000.

[16] Gary L Bostwick. A taxonomy of privacy: Repose, sanctuary, and intimate decision. *California Law Review*, pages 1447–1483, 1976.

[17] Shelley Boulianne. Does Internet Use Affect Engagement? A Meta-Analysis of Research. *Political Communication*, 26(2):193–211, 2009.

[18] Joel Brynielsson, Fredrik Johansson, and Magnus Jändel. Privacy-preserving data mining – A literature review. FOI, the Swedish Defence Research Agency, 2013. FOI-R--3633--SE.

[19] Ann Frances Cameron and Jane Webster. Unintended consequences of emerging communication technologies: Instant messaging in the workplace. *Computers in Human Behavior*, 21(1):85–103, 2005.

[20] Rafael Capurro. Towards an ontological foundation of information ethics. *Ethics and information technology*, 8(4):175–186, 2006.

[21] H. Carlsen, K.H. Dreborg, M. Godman, S.O. Hansson, L. Johansson, and P. Wikman-Svahn. Assessing socially disruptive technological change. *Technology in Society*, 32(3):209 – 218, 2010.

[22] Antonio A Casilli and Paola Tubaro. Why net censorship in times of political unrest results in more violent uprisings: A social simulation experiment on the UK riots. Available at SSRN: http://dx.doi.org/10.2139/ssrn.1909467.

[23] Myriam Dunn Cavelty. Cyber-Terror – Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate. *Journal of Information Technology & Politics*, 4(1):19–36, 2008.

[24] Jeffrey T Checkel. International institutions and socialization in europe: Introduction and framework. *International organization*, 59(04):801–826, 2005.

[25] Francesca Comunello and Giuseppe Anzera. Will the revolution be tweeted? A conceptual framework for understanding the social media and the Arab Spring. *Islam and Christian–Muslim Relations*, 23(4):453–470, 2012.

[26] David Cortright and López George A. *The sanctions decade: assessing UN strategies in the 1990s*. Lynne Rienner Publishers, 2009.

[27] David Cortright and George A López. *Sanctions and the search for security: Challenges to UN action*. Lynne Rienner Publishers, 2002.

[28] Council Regulation (EU) No 36/2012 concerning restrictive measures in view of the situation in Syria and repealing Regulation (EU) No 442/2011. Official Journal of the European Union. The Council of the European Union, 18 January 2012.

[29] Terese Cristiansson and Javier Manzano. Sanktioner bromsar Syriens revolution. Dagens Industri, DI Weekend, 14 September 2012.

[30] Donald Charles F Daniel and Bradd C Hayes. *Coercive inducement and the containment of international crises*. US Institute of Peace Press, 1999.

[31] Michael Dartnell. Insurgency online: Elements for a theory of anti-government internet communications. *Small Wars & Insurgencies*, 10(3):116–135, 1999.

[32] Bertrand de La Chapelle. Multi-stakeholder governance-emergence and transformational potential of a new political paradigm. In *Managing Complexity: Insights, Concepts, Applications*, pages 335–348. Springer, 2008.

[33] Bernhard Debatin, Jennette P Lovejoy, Ann-Kathrin Horn, and Brittany N Hughes. Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, 15(1):83–108, 2009.

[34] Larry Diamond. Liberation technology. *Journal of Democracy*, 21(3):69–83, 2010.

[35] Lee Howell (ed.). Global risks report 2013. World Economic Forum, 2013.

[36] Joshua M Epstein. Modeling civil violence: An agent-based computational approach. *Proceedings of the National Academy of Sciences of the United States of America*, 99(Suppl 3):7243–7250, 2002.

[37] Johan Eriksson. Cyberplagues, IT, and security: Threat politics in the information age. *Journal of Contingencies and Crisis Management*, 9(4):200–210, 2001.

[38] Johan Eriksson and Giampiero Giacomello. The information revolution, security, and international relations:(IR) relevant theory? *International political science review*, 27(3):221–244, 2006.

[39] Mikael Eriksson. *Targeting peace: understanding UN and EU targeted sanctions*. Ashgate Publishing, 2011.

[40] Mikael Eriksson, Ulrik Franke, Magdalena Granåsen, and David Lindahl. Social media and ICT during the Arab Spring. FOI, the Swedish Defence Research Agency, 2013. FOI-R--3702--SE.

[41] Henry Farrell. The consequences of the internet for politics. *Annual Review of Political Science*, 15:35–52, 2012.

[42] Martha Finnemore and Kathryn Sikkink. International norm dynamics and political change. *International organization*, 52(4):887–917, 1998.

[43] Michael Fitzgerald. Predicting Where You'll Go and What You'll Like. http://www.nytimes.com/2008/06/22/technology/22proto.html?_r=1&, June 2080. New York Times, retrieved 15 September 2013.

[44] Luciano Floridi. Information ethics: On the philosophical foundation of computer ethics. *Ethics and information technology*, 1(1):33–52, 1999.

[45] Syrian regime unleashes online propaganda campaign. http://www.france24.com/en/20110613-2011-06-13-1140-wb-en-webnews, June 2011. France24, retrieved 18 January 2013.

[46] Lawrence Freedman. *Strategic coercion: Concepts and cases*. Oxford University Press, 1998.

[47] Lawrence Freedman. Prevention, not preemption. *The Washington Quarterly*, 26(2):105–114, 2003.

[48] Lawrence Freedman. *Deterrence*. Polity Press, Cambridge, 2004.

[49] Leon Fuerth. Cyberpower from the Presidential Perspective. In Franklin D Kramer and Stuart H Starr, editors, *Cyberpower and national security*, pages 557–562. Potomac Books, Inc., 2009.

[50] Karolina Gasinska, Erik Carlson, and Gustaf Salomonsson. ICT and large-scale mobilisation in sub-Saharan Africa. FOI, the Swedish Defence Research Agency, 2013. FOI-R--3703--SE.

[51] Alexander L George, David Kent Hall, and William E Simons. *The limits of coercive diplomacy: Laos, Cuba, Vietnam*. Little, Brown Boston, 1971.

[52] Anindya Ghose and Uday Rajan. The economic impact of regulatory information disclosure on information security investments, competition, and social welfare. In *Fifth Workshop on the Economics of Information Security*, 2006.

[53] Francesco Giumelli. *Coercing, Constraining and Signalling: Explaining UN and EU Sanctions After the Cold War*. ECPR Press, 2011.

[54] Francesco Giumelli. *The Success of Sanctions: Lessons Learned from the EU Experience*. Ashgate Publishing, Ltd., 2013.

[55] Eric Gleave, Howard T Welser, Thomas M Lento, and Marc A Smith. A conceptual and operational definition of'social role'in online community. In *System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference on*, pages 1–11. IEEE, 2009.

[56] N. Hassanpour. Media disruption exacerbates revolutionary unrest: Evidence from Mubarak's natural experiment. In *APSA 2011 Annual Meeting Paper*, 2011. Available at SSRN: http://ssrn.com/abstract=1903351.

[57] Muhammad Aslam Hayat 1. Privacy and islam: From the quran to data protection in pakistan. *Information & Communications Technology Law*, 16(2):137–148, 2007.

[58] Friedrich August Hayek. *The counter-revolution of science*. Free Press Glencoe, 1952.

[59] Francois Heisbourg. A work in progress: the bush doctrine and its consequences. *The Washington Quarterly*, 26(2):73–88, 2003.

[60] David Kurt Herold. Introduction: noise, spectacle, politics: carnival in chinese cyberspace. In David Kurt Herold and Peter Marolt, editors, *Online Society in China: Creating, Celebrating, and Instrumentalising the Online Carnival*, pages 1–20. Routledge, 2011.

[61] Beatrice Heuser. *Western" Containment" Policies in the Cold War: The Case of Yugoslavia, 1948–53*. Routledge, 1989.

[62] Martin Hollis. *The philosophy of social science: an introduction*. Cambridge University Press, 1994. Revised and updated version.

[63] Muzammil M Hussain and Philip N Howard. Democracy's Fourth Wave? Information Technologies and the Fuzzy Causes of the Arab Spring. March 27 2012. Available at SSRN: http://ssrn.com/abstract=2029711.

[64] Emilio Iasiello. Cyber attack: A dull tool to shape foreign policy. In *Cyber Conflict (CyCon), 2013 5th International Conference on*, pages 1–18. IEEE, 2013.

[65] Carl J Jensen. Beyond the tea leaves futures research and terrorism. *American Behavioral Scientist*, 44(6):914–936, 2001.

[66] Shanthi Kalathil and Taylor C Boas. *Open networks, closed regimes: The impact of the Internet on authoritarian rule*. Carnegie Endowment, 2010.

[67] Michael Keane. Broadcasting policy, creative compliance and the myth of civil society in china. *Media, Culture & Society*, 23(6):783–798, 2001.

[68] Ali Khoshgozaran and Cyrus Shahabi. A taxonomy of approaches to preserve location privacy in location-based services. *International Journal of Computational Science and Engineering*, 5(2):86–96, 2010.

[69] Gary King, Jennifer Pan, and Molly Roberts. How censorship in China allows government criticism but silences collective expression. In *APSA 2012 Annual Meeting Paper*, 2012. Available at SSRN: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2104894.

[70] Brian S. Krueger. Assessing the potential of internet political participation in the united states: A resource approach. *American Politics Research*, 30(5):476–498, 2002.

[71] Johan Lagerkvist. Principal-Agent Dilemma in China's Social Media Sector? The Party-State and Industry Real-Name Registration Waltz. *International Journal of Communication*, 6:2628–2646, 2012.

[72] Johan Lagerkvist and Gustav Sundqvist. Loyal Dissent in the Chinese Blogosphere: Sina Weibo Discourse on the Chinese Communist Party. *Studies in Media and Communication*, 1(1):p140–149, 2013.

[73] John Lang and Hans De Sterck. The Arab Spring: A Simple Compartmental Model for the Dynamics of a Revolution. *arXiv preprint arXiv:1210.1841*, 2012.

[74] Marc Langheinrich. A privacy awareness system for ubiquitous computing environments. In *UbiComp 2002: Ubiquitous Computing*, pages 237–245. Springer, 2002.

[75] Richard Ned Lebow. *Why Nations Fight: Past and Future Motives for War*. Cambridge University Press, 2010.

[76] Kyumin Lee, James Caverlee, Zhiyuan Cheng, and Daniel Z Sui. Content-driven detection of campaigns in social media. In *Proceedings of the 20th ACM international conference on Information and knowledge management*, pages 551–556. ACM, 2011.

[77] Kyumin Lee, Prithivi Tamilarasan, and James Caverlee. Crowdturfers, Campaigns, and Social Media: Tracking and Revealing Crowdsourced Manipulation of Social Media. In *Proceedings of the 7th International AAAI Conference on Weblogs and Social Media*. AAAI, 2013.

[78] Lawrence Lessig. New chicago school, the. *J. Legal Stud.*, 27:661, 1998.

[79] James Andrew Lewis. *Assessing the risks of cyber terrorism, cyber war and other cyber threats*. Center for Strategic & International Studies, 2002.

[80] Bin Liang and Hong Lu. Internet development, censorship, and cyber crimes in china. *Journal of Contemporary Criminal Justice*, 26(1):103–120, 2010.

[81] Martin C Libicki. *Cyberdeterrence and cyberwar*. Rand Corporation, 2009.

[82] Martin C. Libicki. Don't buy the cyberhype. *Foreign Affairs*, 2013. http://www.foreignaffairs.com/articles/139819/martin-c-libicki/dont-buy-the-cyberhype?page=show, accessed August 20, 2013.

[83] Markku Lonkila. The Role of Social Media in the Ruling of Russia. Presentation at the conference Russia's Winter of Discontent: Taking Stock of Changing State-Society Relationships, Uppsala, Sweden, September 7, 2013.

[84] Michael S Lund. *Preventing Violent Conflicts: A Strategy For Preventive Diplomacy Author: Michael S. Lund, Publisher: United States Insti*. United States Institute of Peace Press, 1996.

[85] Ringo Ma. Spread of SARS and war-related rumors through new media in China. *Communication Quarterly*, 56(4):376–391, 2008.

[86] Rebecca MacKinnon. China's "networked authoritarianism". *Journal of Democracy*, 22(2):32–46, 2011.

[87] Kevin Macnish. Unblinking eyes: the ethics of automating surveillance. *Ethics and information technology*, 14(2):151–167, 2012.

[88] Peter Marolt. Grassroots agency in a civil sphere? In David Kurt Herold and Peter Marolt, editors, *Online Society in China: Creating, Celebrating, and Instrumentalising the Online Carnival*, pages 53–67. Routledge, 2011.

[89] John J Mearsheimer. *Conventional deterrence*. Cornell University Press Ithaca, 1983.

[90] Masahiko Mizutani, James Dorsey, and James H Moor. The internet and japanese conception of privacy. *Ethics and Information Technology*, 6(2):121–128, 2004.

[91] Mohamed Nanabhay and Roxane Farmanfarmaian. From spectacle to spectacular: How physical space, social media and mainstream broadcast amplified the public sphere in Egypt's 'Revolution'. *The Journal of North African Studies*, 16(4):573–603, 2011.

[92] National Intelligence Council. Global Trends 2030: Alternative Worlds. http://www.dni.gov/index.php/about/organization/national-intelligence-council-global-trends, accessed February 25, 2013, December 2012.

[93] Lars Nicander. Shielding the net – understanding the issue of vulnerability and threat to the information society. *Policy Studies*, 31(3):283–300, 2010.

[94] Leysia Palen and Paul Dourish. Unpacking privacy for a networked world. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 129–136. ACM, 2003.

[95] Andreas Pfitzmann and Marit Köhntopp. Anonymity, unobservability, and pseudonymity—a proposal for terminology. In *Designing privacy enhancing technologies*, pages 1–9. Springer, 2001.

[96] Barbara Poblete, Myra Spiliopoulou, and Ricardo Baeza-Yates. Website privacy preservation for query log publishing. In *Privacy, Security, and Trust in KDD*, pages 80–96. Springer, 2008.

[97] Clara PORTELA SAIS. The EU Sanctions against Syria: Conflict Management by other Means? *Egmont Security Brief*, 36, 2012.

[98] Stephen Prentice and Gyanee Dewnarain. The Future of the Internet: Fundamental Trends, Scenarios and Implications to Heed. Technical report, Gartner, Inc., August 2012. Report no. G00237004.

[99] Anas Qtiesh. Spam Bots Flooding Twitter to Drown Info About [Hashtag]Syria Protests. http://advocacy.globalvoicesonline.org/2011/04/18/spam-bots-flooding-twitter-to-drown-info-about-syria-protests/, april 2011. Global Voices Online, retrieved 18 January 2013.

[100] Jacob Ratkiewicz, Michael Conover, Mark Meiss, Bruno Gonçalves, Snehal Patil, Alessandro Flammini, and Filippo Menczer. Detecting and tracking the spread of astroturf memes in microblog streams. *arXiv preprint arXiv:1011.3768*, 2010.

[101] Jacob Ratkiewicz, Michael Conover, Mark Meiss, Bruno Gonçalves, Snehal Patil, Alessandro Flammini, and Filippo Menczer. Truthy: mapping the spread of astroturf in microblog streams. In *Proceedings of the 20th international conference companion on World wide web*, pages 249–252. ACM, 2011.

[102] Tapas Ray. The'story'of digital excess in revolutions of the arab spring. *Journal of Media Practice*, 12(2):189–196, 2011.

[103] Internet enemies report 2012. Reporters Without Borders, March 2012.

[104] Reuters. China threatens tough punishment for online rumor spreading. http://www.reuters.com/article/2013/09/09/us-china-internet-idUSBRE9880CQ20130909. Published September 9, 2013, retrieved October 18 2013.

[105] Hal Roberts, Ethan Zuckerman, Jillian York, Robert Faris, and John Palfrey. 2010 circumvention tool usage report. Technical report, The Berkman Center for Internet & Society, October 2010.

[106] David Robertson. *A dictionary of modern defence and strategy*. Europa Publications Limited, London, 1987.

[107] Devan Rosen, Jang Hyun Kim, and Yoonjae Nam. Birds of a feather protest together: theorizing self-organizing political protests with flock theory. *Systemic practice and action research*, 23(5):419–441, 2010.

[108] Julie J.C.H. Ryan, Daniel J. Ryan, and Eneken Tikk. Cybersecurity regulation: Using analogies to develop frameworks for regulation. In Eneken Tikk and Anna-Maria Talihärm, editors, *International Cyber Security Legal & Policy Proceedings*, pages 76–99. Cooperative Cyber Defence Centre of Excellence (CCD COE), Tallinn, 2010.

[109] Kristin Zahra Sands. Muslims, identity and multimodal communication on the internet. *Contemporary Islam*, 4(1):139–155, 2010.

[110] Frank Schimmelfennig, Stefan Engert, and Heiko Knobel, editors. *International socialization in Europe: European organizations, political conditionality and democratic change*. Basingstoke: Palgrave Macmillan, 2006, 2006.

[111] Frank Schimmelfennig and Ulrich Sedelmeier. *The politics of European Union enlargement: theoretical approaches*. Routledge, 2005.

[112] Zhangwen Tan, Xiaochen Li, and Wenji Mao. Agent-based modeling of netizen groups in Chinese internet events. In *Intelligence and Security Informatics*, pages 43–53. Springer, 2011.

[113] Edward Tenner. *Why things bite back: Technology and the revenge of unintended consequences*. Vintage, 1997.

[114] Thien A. Tran and Tugrul Daim. A taxonomic review of methods and tools applied in technology assessment. *Technological Forecasting and Social Change*, 75(9):1396 – 1405, 2008.

[115] Gregory F Treverton. *Reshaping national intelligence for an age of information*. Cambridge University Press, 2001.

[116] Peter Wallensteen, Carina Staibano, and Mikael Eriksson. Routes to Democracy in Burma/Myanmar: The Uppsala pilot study on dialouge and international strategies. 2004.

[117] Samuel D Warren and Louis D Brandeis. The right to privacy. *Harvard law review*, 4(5):193–220, 1890.

[118] Frank C Zagare and D Marc Kilgour. *Perfect deterrence*. Cambridge University Press (New York), 2000.

[119] Jinqiu Zhao. A snapshot of Internet regulation in contemporary China: Censorship, profitability and responsibility. In Friederike Assandri and Dora Martins, editors, *From Early Tang Court Debates to China's Peaceful Rise*, pages 141–151. Internet Society of China, 2009.

[120] Giovanni Ziccardi. *Resistance, liberation technology and human rights in the digital age*. Springer, 2013.

FOI, Swedish Defence Research Agency, is a mainly assignment-funded agency under the Ministry of Defence. The core activities are research, method and technology development, as well as studies conducted in the interests of Swedish defence and the safety and security of society. The organisation employs approximately 1000 personnel of whom about 800 are scientists. This makes FOI Sweden's largest research institute. FOI gives its customers access to leading-edge expertise in a large number of fields such as security policy studies, defence and security related analyses, the assessment of various types of threat, systems for control and management of crises, protection against and management of hazardous substances, IT security and the potential offered by new sensors.

FOI
Swedish Defence Research Agency
SE-164 90 Stockholm

Phone: +46 8 555 030 00
Fax: +46 8 555 031 00

www.foi.se