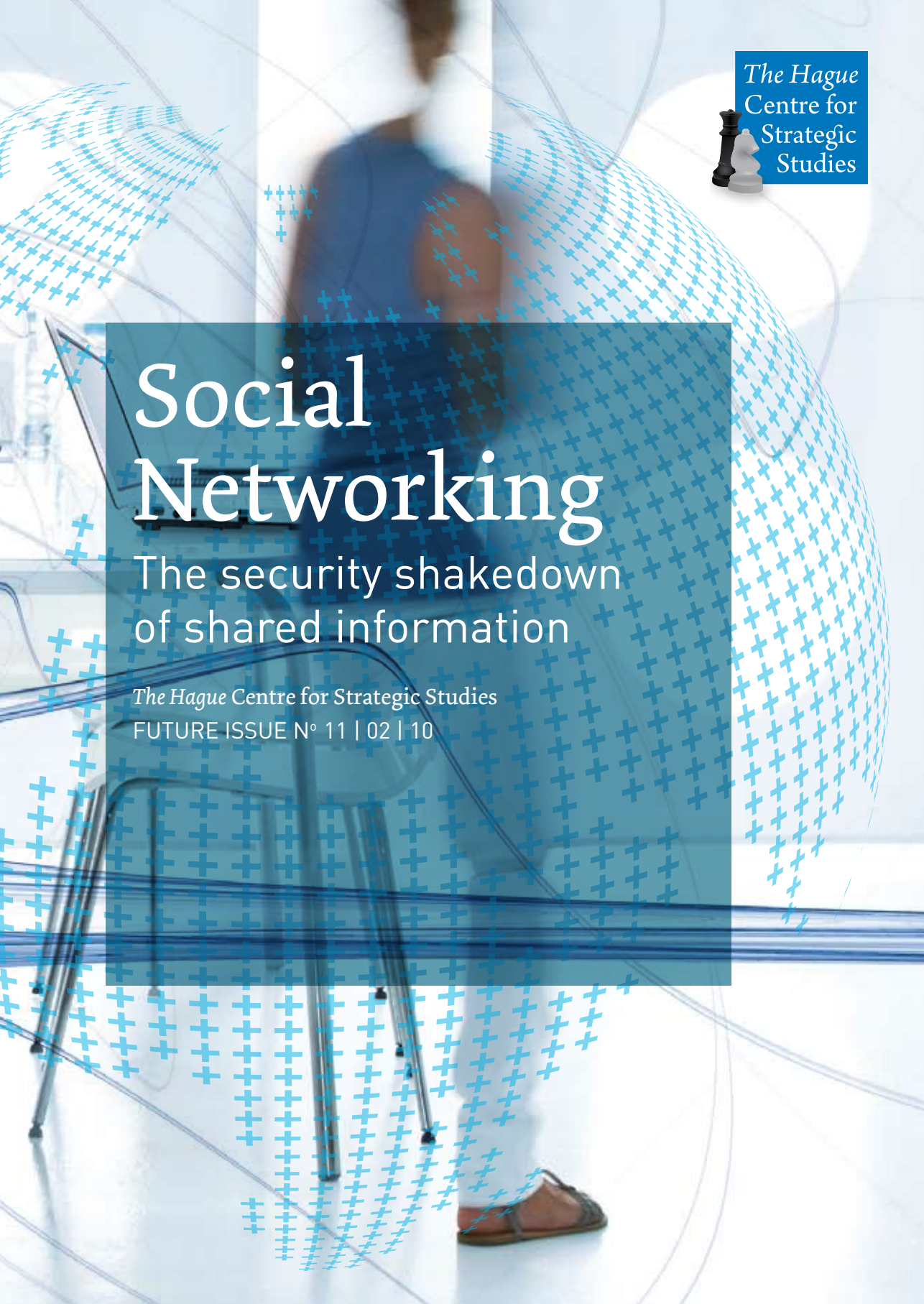

The Hague Centre for Strategic Studies

Social Networking

The security shakedown of shared information

The Hague Centre for Strategic Studies
FUTURE ISSUE N° 11 | 02 | 10

The Hague Centre for Strategic Studies (HCSS) seeks to advance international security in an era defined by geopolitical, technological and doctrinal transformation and new security risks. HCSS provides strategic analysis and offers concrete policy solutions to decision makers. HCSS serves as a strategic planning partner to governments, international organisations and the business community.

Social Networking
The security shakedown of shared information
The Hague Centre for Strategic Studies

Aksel Ethembabaoglu, Tim Sweijs, George Boone, Kevin Goreham and Stephan de Spiegeleire

Graphic Design *Studio Maartje de Sonnaville, The Hague*

The Hague Centre
for Strategic Studies

Lange Voorhout 16
2514 EE The Hague
The Netherlands

info@hcss.nl
www.hcss.nl

Social Networking

The security shakedown of shared information

The Hague Centre for Strategic Studies
FUTURE ISSUE Nº 11 | 02 | 10

Table of Contents

In brief

In recent years, social networks have emerged as popular Web 2.0 applications. This has profound implications for the security realm. The Hague Centre for Strategic Studies (HCSS) reviewed the nascent debate within the security foresight community on this new phenomenon and has uncovered four key security implications of social networks:

Information Security: Social networks may, unintentionally, jeopardise information security. Social networks facilitate information security risks such as privacy infringement, corporate espionage, and the spread of malware. These risks will likely be exacerbated by the increased use of social networks by individuals, organisations and governments.

Information Dissemination: Social networks introduce a new distributed and decentralised mode of communication which has only started to be explored by governments, businesses corporations, and other non-governmental organisations. An increasing number of the studies on social networks examine the role of social networks in strategic government communication which in turn may impact strategic decision-making processes on security. For example, social networks may shorten the OODA-loop (Observe, Orient, Decide, Act) because it allows for faster decision-making using novel methods for communication. Social networks may strengthen democracy by facilitating the free flow of information and increasing transparency of government actions (thereby shifting power away from governments to populations). However, they may undermine democracy by providing a platform for conspiracy theories whose origins and claims may be more difficult to verify for the average citizen.

Intelligence Operations: Social networks are used by individuals, corporations and government agencies to collect intelligence in various formats, such as individuals' personal details and personal histories, their employment details and employment histories and their social relations, as well as on product

information, consumer behaviour and more. This may, on the one hand, strengthen the ability of governments to monitor the behaviour of citizens while, on the other hand, it may strengthen the position of non-state actors in relation to state governments. Intelligence operations on social networks in the future may provide novel ways for individuals to influence governmental intelligence by strategically placing false information, creating deceptions, or by hacking government systems using social networks.

Organisational Capabilities: Social networks may provide a powerful tool for groups of people to self-organise. This has already been demonstrated in a number of revolutions and uprisings over the past few years. Social networks' potential to mobilise people is not restricted solely to the political domain nor is it limited to any particular geographical boundaries, and it is expected that its use will spread further in the future.

Table 1 gives an overview of the drivers, parameters and security implications of social networks that were identified in the foresight community's existing literature.

DRIVERS	PARAMETERS	SECURITY IMPLICATIONS
Accessibility	Network Organisation	Information Security
Benefits	Ubiquity of Social Networks	Information Dissemination
User Data Availability	Technical Architecture	Intelligence Operations
Security	Trust	Organisational Capabilities
Privacy	Quality of Information	
Trust	Security Defences	
Bandwidth		

Table 1. OVERVIEW OF THE DRIVERS, PARAMETERS AND SECURITY IMPLICATIONS OF SOCIAL NETWORKS IDENTIFIED IN THE FORESIGHT COMMUNITY'S DISCOURSE

1 Introduction

In the past year, social networking applications have demonstrated the ability to influence major events. Most recently, Twitter, a micro-blogging tool, played a major role in the upheaval following the 2009 Iranian election crisis.[1] Following the disputed victory of president Ahmadinejad, massive protests erupted throughout Iran. Traditional state methods to control the media failed to prevent the leakage of domestic information abroad as Iranians used social networks to circumvent political censorship.[2]

Social networking applications facilitate the creation and dissemination of user-generated content because they allow anyone with an internet connection to create and post content which can be viewed in real-time by interested groups. Through social networks, individuals generate and share information and in so doing, increase knowledge on an issue. Consequently, the number of users impacts the effectiveness of a social network because additional users contribute additional information to a knowledge base.

Social networks have taken the virtual world by storm in recent years. Facebook, for example, a popular social networking application, has averaged an annual increase of 70 million members since its inception and has expanded by a factor of 28 since 2007 (see Figure 1).[3] Such enormous growth rates lead to more information becoming more quickly available to many more users. As a result, social networking applications are becoming increasingly effective as an information facilitator because of the growing amount of user-generated content for a greater number of users.

The security realm has not remained immune from the increased influence of social networks. For instance, in mid-2009, the wife of Sir John Sawers, the current British Secret Intelligence Service Chief, posted personal information on Facebook resulting in a nationwide debate on online security.[4]

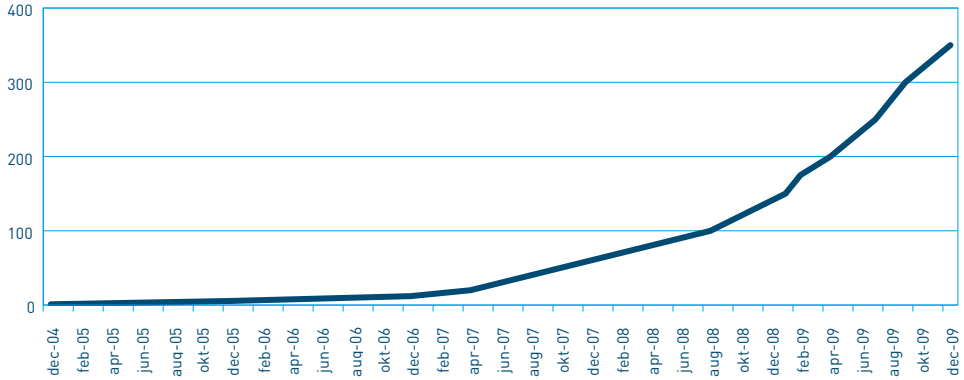

Figure 1. FACEBOOK MEMBERSHIP 2004-2009, IN MILLIONS OF USERS

The aforementioned anecdote is just one example of the multiple security implications of social networks. In an increasing number of areas, social networks pose a growing risk to information security, bring forth novel methods of information dissemination, intelligence collection and, lastly, reshape organisational activities. As such, it is likely that social networks will increasingly and substantially impact the security landscape of the 2010s.

2 Social networks: an overview

HCSS conducted a meta-analysis of foresight studies describing social networks. Despite being a relatively new phenomenon over 60 relevant foresight studies have been published on this issue by experts working at the crossroads of information technology, security and future studies. Figure 2 illustrates the increasing number of reports on social networks suggesting a growing interest in the topic. An analysis of these foresights yielded the following aggregate view (see Figure 3) of the most important parameters, drivers and security implications identified by the foresight community.* Figure 4 and Figure 5 provide more detailed overviews of references to the parameters and drivers in the foresight discourse. As depicted in the graph of Figure 3, many of the parameters and drivers of social networking are closely interrelated.

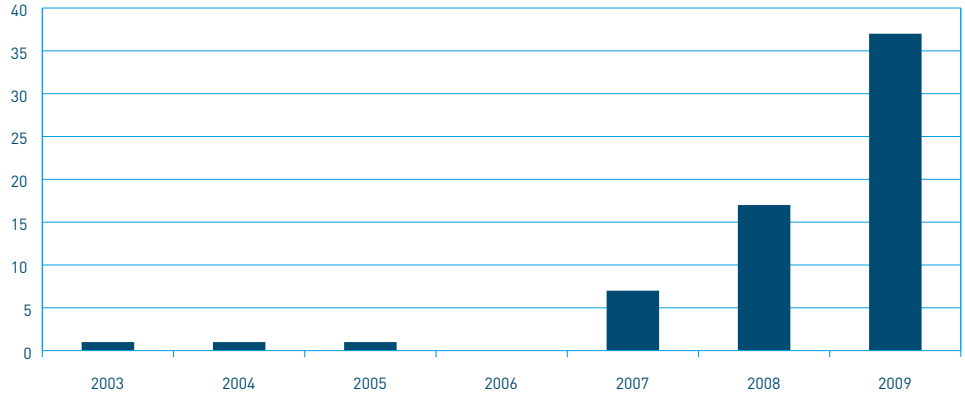

Figure 2. NUMBER OF FORESIGHT REPORTS ON SOCIAL NETWORKING

* Figure 3 depicts only the paramount drivers, parameters and implications. A full explanation and operationalisation of the identified drivers, parameters and implications are provided in Appendix I.

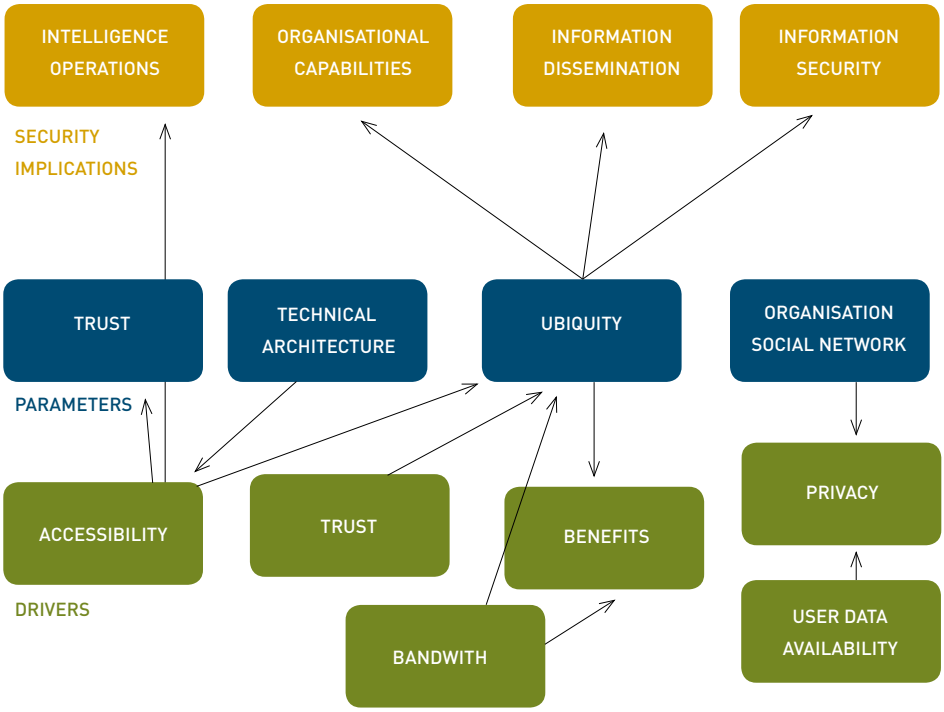

Figure 3. PARAMOUNT DRIVERS, PARAMETERS AND SECURITY IMPLICATIONS

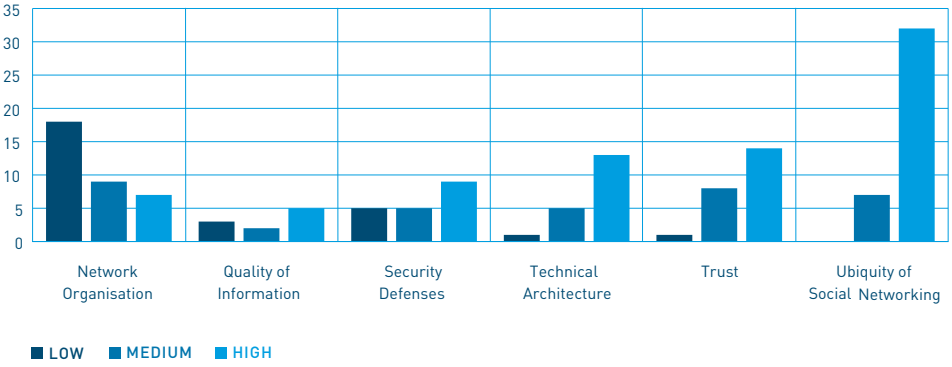

Figure 4. OVERVIEW OF SOCIAL NETWORKING PARAMETERS AND THEIR FREQUENCY*

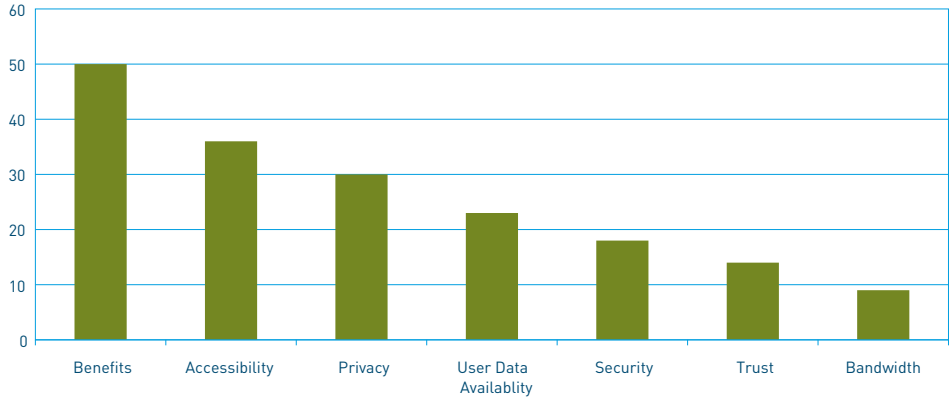

Figure 5. OVERVIEW OF SOCIAL NETWORKING DRIVERS AND THEIR FREQUENCY

* The classification for low, medium, high does not apply to each of the parameters. In Network Organisation the disparity is labeled as niched, hybrid, central. In technical architecture, a distinction is made between centralised, hybrid and decentralised architectures.

The foresight community generally holds that future social networks will be characterised by *highly decentralised technical architectures*, meaning that such architectures are not proprietary or centrally localised and hosted. Decentralised architectures allow a large distributed network to take shape, increasing the accessibility and, consequently, the information dissemination capabilities of social networks, for example by introducing a single login account for all social network sites instead of requiring users to rely on multiple accounts.

If advanced social networking tools are available nearly 24/7 to many users, on the basis of recent developments in the open source innovation domain HCSS assesses this will fuel further innovation and capabilities of real time communication programmes available on the web.

The *ubiquity of social networks*, the level of penetration of social networks into everyday life, is also expected to see a marked increase in the future. The social penetration of social networks is dependent on, among other factors, accessibility, bandwidth and trust, where trust is akin to a belief in the benignity of, and a level of familiarity with, social networks. In turn, this introduces novel ways in which information may be compromised thus making the importance of information security more paramount. Additionally, the increasing omni-presence of social networks also stimulates potential benefits to be derived from participation in social networks.

HCSS assesses that the design of social networking applications and the membership using them will closely keep track with user-preferences in order to increase trust. Social networking sites will continue and increase their user-profiling operations to completely identify and map user-preferences. According to the combined parameters and drivers' meta-analysis, this studying of user-preferences will likely produce niche applications that provide advanced solutions to users' specific requirements.

Furthermore, user *trust* in social networks is expected to continue to grow strongly into the future. The increased accessibility to social networks, as they permeate throughout everyday life, impacts the level of familiarity users develop for social networks. Users will use social networks to gather and collect information about a larger number of issues. As a result, and perhaps indirectly, user trust in social networks will increase.

Many authors believe that the *organisational structure of social networks*, either a proprietary central social network or a decentralised specialised social network, will exhibit a niche-like decentralised structure rather than being a central portal. Profilactic and Google's Socialstream are examples of a series of applications using a portal-like structure which resemble social networks. According to their website, Profilactic is a "social media aggregator/ lifestreaming service that pulls together just about everything you and your friends create online".[5] Although Profilactic does not constitute a single company offering a variety of services, it does provide an example of an attempt to aggregate or centralise social networks. However, the majority of authors on this subject believe that the future lies in niche-like applications such as Last.fm (a social network site that specialises in sharing music preferences), Facebook (a social network for keeping in touch with friends) or LinkedIn (a career site used to share job information). The specialisation of social networks is similar to the ways in which businesses tend to specialise in the marketplace in order to compete. Various businesses produce multiple advanced and tailored products rather than a single company producing everything for everyone. However, specialisation and competition may also have its drawbacks. It is expected that niche social networks will push the limits of user privacy as tailored services require increasingly more user information to identify user preferences and remain competitive. This may result in an increasing number of privacy infringements and eventually test the limits of privacy regulation.

3 Security implications

The drivers and parameters of social networks noted in the previous section produce a number of security implications. The security implications' meta-analysis (see Figure 6) identifies the following dominant themes: *Information Security*, *Information Dissemination*, *Intelligence Operations* and *Organisational Capabilities*. HCSS expands on each of these implications in the following paragraphs.

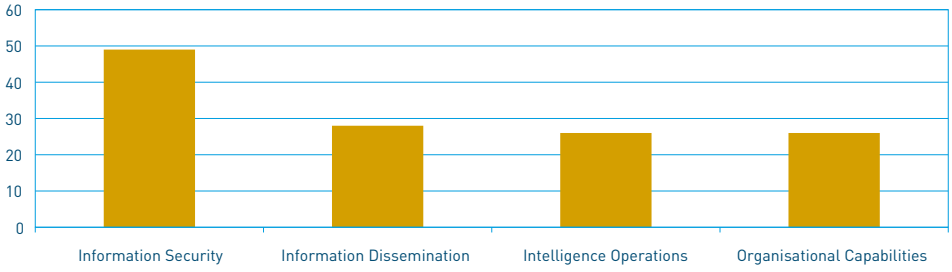

Figure 6. META-ANALYSIS SOCIAL NETWORKING SECURITY IMPLICATIONS AND THEIR FREQUENCY

3.1 Information Security

Social networks may threaten the privacy of users and the security of corporate information if these are not properly guarded. With the increasing ubiquity of social networks in tomorrow's world, information becomes vulnerable to security breaches. Reports indicate that in 2009, nineteen percent of all kinds of hacking attacks targeted social networking sites, thus illustrating the emergence of a new security threat.[6] Analytically speaking, there are two types of threats to information security.

First, the security of information on individuals and organisations may be compromised through the loss of control over data. For example, contrary to his/her wishes, a user's name, address, job and telephone number might be publicly available on the internet. It certainly appears that social network users have limited control over their profile data. For instance, on the social network site Facebook, people are 'tagged' by other users (e.g. names can be attributed to faces in pictures) even if they are not Facebook members themselves.[7] Users are often not aware of the amount of personal information that is available on social networks nor how easily it can be misused through identity theft. This security risk will increase as societies continue to digitalise.[8] There are many examples of personal information being misused for attempts at fraud, including the distribution of unsolicited e-mails, the instalment of key logging software (i.e. to steal passwords) and large scale phishing attempts, (acquiring sensitive information by acting as a trustworthy source, e.g. as a bank).[9]

The exposure of sensitive data to others does not only affect individual users but also extends to organisations. Businesses organisations run the risk of losing control over information that is vital to their economic competitiveness (e.g. confidential product information). As employees increasingly use social networking services, more and more companies' information is openly available than may be deemed desirable for them. Organisations may find their infrastructure is easily exposed as a result of information retrieved from social networks. Using LinkedIn, for instance, employees post detailed information of the structure of their organisations as they customise their profiles.[10] This sort of information may contain overviews of departments, recent promotions and job transfers, or other events that reveal the inner workings of an organisation. Furthermore, organisations can seriously suffer from digital attacks on their reputation. Public comments or other user-generated information may embarrass a company through negative feedback, inappropriate remarks or the leaking of sensitive information. These are not merely hypothetical situations. In a recent case, a Microsoft employee placed valuable information on his LinkedIn profile that indicated strategic decisions and developments at Microsoft.[11] Such leaks can even result in corporate intellectual property getting lost or stolen. For governmental organisations, the loss of control over information can be just as damaging because of its public function. In the Netherlands, for example, an employee of the Military Intelligence and Security Service (MIVD) posted information on LinkedIn about his professional activities, revealing internal agency processes.[12] Dutch journalists were keen to expose these

weaknesses arguing that employees of these institutions require training in using online social network applications. It remains unclear how damaging this publicly available information was to the MIVD but, nonetheless, for a government agency mandated specifically to gather intelligence and to conduct clandestine activities such a leak is, at the very least, embarrassing.

The second threat to information security is the threat of data being compromised. Attacks on ICT security infrastructures often rely on so-called malware. Malware is hidden malicious software that can infiltrate, manipulate or damage data on a computer. Its spread is often facilitated by other Web 2.0 applications like embedded blogs or YouTube videos that are seamlessly integrated into social networks. Due to shared user-generated communication on social networks, malware can quickly and easily spread among a large number of users and occur both in overt and covert modes – in that social network users may unknowingly contribute to the spread of malware. This is precisely what happened on the social network site MySpace, when malware spread through Flash movies embedded on personal profile sites and affected up to 100,000 MySpace accounts that were used as slave computers for 'botnets'.[13] A botnet can be visualised as a digital crowd of zombies relentlessly and endlessly performing assigned actions, such as breaking a password by repeatedly trying new password letter combinations. Alternatively, malware can be introduced through cross-site scripting. Cross-site scripting is when hackers bypass website security mechanisms by injecting malicious code into web pages.

In addition, hackers have used social networks to connect people and data by impersonating a friend and spreading links to dangerous websites that contain or inject dangerous software codes such as the "Koobface" virus.[14] Targeted computers may be seized by hackers using social networks either by controlling targeted computers through injected malicious code or by obtaining sensitive login data through social engineering, which is the act of manipulating people into performing actions or divulging confidential information. Using their acquired illicit access, hackers may be able to disable government websites, infiltrate organisations or steal sensitive information. Alternatively, they may disrupt frequently used internet services such as online payments.

3.2 Information Dissemination

Social networks facilitate the creation on new online content by sharing information between individuals and organisations. This interaction may shape

the conduct of future (strategic) communication. Social networks provide individuals with the ability to rapidly disseminate information worldwide. Disseminating information through social networks is a powerful tool for organisations because it may optimise strategic communication and improve decision-making. New means of communication offer organisations entirely new dimensions through which they can operate. Four organisational methods for information sharing are identified by Drapeau and Wells which provide a useful framework to discuss the ways in which information may be disseminated through social networks. These methods are: *(1) inward sharing*, *(2) outward sharing*, *(3) inbound sharing* and *(4) outbound sharing*.[15]

Inward and *outward* sharing relate to sharing organisational information within the organisation or outside with direct partners. Inside an organisation, increased coordination and collaboration can be fostered between various departments through the use of social networks to allow smoother data sharing and processing, for instance through the use of a Wiki on a specific topic moderated by individuals of different departments. Similarly, an organisation might host a personalised group page on a social network site such as LinkedIn. Alternatively, organisations can optimise coordination with external partners, sharing relevant information with partner organisations such as sister-agencies, non-governmental organisations or other corporations. This type of information sharing was effectively implemented through the secure military forum CAVNET.[16] Using CAVNET, U.S. military officers in Iraq shared information on the quickly changing insurgent tactics in addition to regular military reports. This allowed the military officers to effectively adapt their strategies to successfully combat the latest insurgent tactics.

Inbound and *outbound* sharing describes information that is received by an organisation about other parties whether individuals or external organisations. For example, inbound sharing may refer to customer comments on certain products that are collected by a corporation through the use of social networks. Not only businesses but also national and local governments are becoming increasingly open to outside input. More and more, citizens are given digital platforms to communicate with their governments. For example, local governments can use Wikis to identify the needs of citizens as users actively contribute to formulating, and thus shape, the debates on issues.[17]

With outbound sharing, organisations use social media to share governmental information with external sources, such as responses to inquiries or adjusted policies based on citizen input. In this vein, social networks are increasingly used as a political propaganda tool. During the recent Gaza conflict, Israel used Twitter to influence public opinion.[18] But outbound sharing also includes politicians that communicate, inform and engage with their constituents through an online presence in a social network.[19]

The aforementioned methods of information sharing may have even greater security implications because they indicate a transformation from traditional to new media. Traditionally, the media was used by both citizens and governments to stay informed and thus influenced public opinion. However, with the distributed approach (empowering many individuals rather than power centres) of social media to generate content, these diverse loci of information may replace the traditional media in its role of government watchdog. Previously, for example, journalists would be sent to the field to monitor government actions and their report was then printed in a newspaper. Arguably, this increased the likelihood that a reporter might be misled or altogether miss a story. However, with the advent of social media, any individual with a social network account can report government actions thus turning the entire population into a network of "mini"-watchdogs as demonstrated by the 2009 Iranian election fallout. Traditional media outlets are unlikely to disappear in the near future but their role will change. In all likelihood, they will increasingly function more as editors than authors *per se*, reducing and sifting the voluminous amount of information from new social media. This emergence of this distributed individual empowerment increases the power of populations vis-à-vis their governments because it potentially reduces governments' influence on public opinion. Most notably, the power of oppressive regimes may deteriorate as they lose control of information dissemination. However, at the same time, such regimes might attempt to dilute such effects by using social networks themselves to disseminate false or misleading information.

The empowerment of individuals may prove equally useful for consumers as it does for large corporations because they can inform consumer groups to either support or block products or corporate policies. Although the actual impact remains to be seen, social networks have the potential to support democracy (more people are empowered) and transparency (corporate and government actions are not easily covered up). Yet, social networks may also fuel

unsubstantiated 'conspiracy theories', thereby affecting the quality of information – so vital to informed debate – and, arguably, undermining one of the core pillars of democracy. Two recent examples of this phenomenon are the rumour that death squads would be part of the health care plans of president Obama, an allegation that was first posted by former GOP vice-presidential contender Sarah Palin on her Facebook page; and European discussions on the use and utility of human papillomavirus vaccines, sparked by national vaccine campaigns across Europe, which were plagued by mal-informed assertions that spread through social networks.[20] These examples illustrate how social networks may strengthen the hand of non-state actors, serve as a detractor to the status of 'expert opinion', and derail the capacity of national governments to implement national policies.

3.3 Intelligence Operations

Governments and businesses alike monitor social networks to expand their intelligence collection capabilities. The collection of intelligence through social networks may serve as a force multiplier because it could contribute to improved decision-making. For intelligence collection, sophisticated algorithms take snapshots of social networks to monitor user behaviour and the development of social relations. One such example is the Social Network Analysis (SNA) which is used by government agencies to track terrorist networks. It has become a well-regarded and popular intelligence analysis tool.[21]

Businesses also monitor social relations to improve their business operations and so to increase competitiveness. For example, businesses may seek to determine user preferences for targeted advertising using social networks. One method for targeted advertising is user-profiling which collects a user's online information to generate customised user preferences. For example, Facebook used its Beacon service to track activities of users in third-party partner sites.[22] Furthermore, employers are increasingly using social networks for vetting purposes and to verify track records.[23] These developments may lead to an increasingly deterministic future. If social networking use keeps increasing, future consumers and citizens are likely to be monitored from an early age thus providing a plethora of data for analysis and profiling. Although initially useful with the automated provision of, for example, restaurant suggestions tailored to a user's preference, in the longer-term, this technology could just as well prevent users from getting a job, a subscription or medical care because they are identified and profiled as either unqualified, unhealthy, a safety risk or possibly

a terrorist. The continuous development of improved intelligence collection and analysis may pose serious challenges to the privacy and personal opportunities of future generations.

Governments and businesses also actively generate information and social relations on social networks to gather intelligence. They may engage and manipulate social networks in order to edge into a specific web of social relations thus adding another way to collect intelligence (e.g. by imposing as another user and becoming 'friends' with targets such as suspected terrorists, or, by controlling an entire social network sites altogether). This is perhaps most worrisome for large and rigid organisations which might have difficulty in adapting organisational policies and developing the necessary capabilities quickly enough to respond both offensively and defensively to these new technologies. Nonetheless, governments are already actively engaged in this type of intelligence collection. For example, in 2008, North Korea allegedly tried to infiltrate the South Korean military by linking up and creating online relations with South Korean military officers.[24]

3.4 Organisational Capabilities

Social networking sites may facilitate the mobilisation of large groups of people for strategic leaders. Strategic leaders which can leverage social networking capabilities can be found among government leaders, captains of industry, terrorist leaders and specific individuals. A good example of a public figure using the organisational potential of social networks is U.S. President Barack Obama in his electoral campaign. President Obama utilised social networks such as Facebook Groups and a LinkedIn profile to engage with citizens.[25] In turn, through these social network sites, he was able to mobilise individuals and raise campaign funds in new ways and on an unprecedented scale.[26] In contrast to previous elections, in this case, President Obama empowered individuals by distributing, power, both financial and voting thus reducing his dependency on traditional, centralised sources of political power and corporate interest groups. Similarly, in Egypt, two students protested against their government's policies by starting a Facebook Group. Within days, the group attracted approximately 40,000 members and subsequently, still using Facebook, they organised a demonstration that surprised state security agents because of the unexpectedly high number of participants.[27] This case also illustrates the decentralising and distributing impact social networks have had on contemporary mobilisation capabilities by empowering individuals.

These examples of political mobilisation examples illustrate a profound change in organisational practices. With the emergence of an increasing amount of social networking applications, organisational practices through social networks are likely only to gain in power because of an increasing number of users that can be organised through social networks. Social networks continue to spread to mobile devices thus further increasing their accessibility and ubiquity. This not only allows mobilisation of the masses on a strategic level for political activism (e.g. by posting protest dates and locations or garnering an online presence), but also on an operational level, by directly communicating during a protest with real-time micro-blogging tools like Twitter. For example, when rumours on Twitter suggested that the President of Madagascar allegedly sought refuge in the U.S. embassy in Antananarivo, the U.S. State Department was quick to send 'tweets' to deny the rumour, fearing the rapid mobilisation of opposition supporters using Twitter to storm the U.S. embassy which was open.[28]

Despite being frequently cited in the media, political activists do not have a monopoly on the ability to mobilise and organise people using social networks. Crowdsourcing, outsourcing the generation of issue-specific solutions to a crowd or group of people through an open call, is a broader emerging phenomenon. In researching the potential for mobilising people to a non-political cause, the United States Defense Advanced Research Projects Agency (DARPA) organised a contest (with a $40.000 reward) to locate 8 red balloons spread throughout the country using online social networks. In so doing, it sought to test the ability of non-political social network groups to provide timely communication, to work effectively as a team across a wide area and to mobilise resources quickly, which are prerequisites to solving broad-scope, time-critical problems. The test succeeded: the solution was generated in less than nine hours.[29]

4 Insights in social networks

Social networks have played, and will continue to play, an important role in the future. The foresight community has already touched upon numerous security implications of the rise of social networks. A brief overview of these implications is listed in Table 2.

KEY ISSUES	INDIVIDUALS	ORGANISATIONS (E.G. BUSINESSES OR NGOS)	GOVERNMENTS
INFORMATION SECURITY	User-profile determinism	Susceptibility to corporate espionage, growing number of ICT security breaches	Susceptibility to intelligence agency espionage, growing number of ICT security breaches
INFORMATION DISSEMINATION	Increased individual empowerment due to distributed and decentralised power nodes	Tool for strategic communication, improved decision-making, improved intra-and interorganisation cooperation, consumer empowerment vis-à-vis large corporations	Tool for strategic communication, improved decision-making, improved intra- and interorganisational cooperation, novel means for government propaganda, increased citizen input and empowerment resulting in increased transparency and more effective democracy
INTELLIGENCE OPERATIONS	Loss of control over personal data, increasing vulnerability to unauthorised personal information collection, information manipulation	Tool for employee vetting, increasing corporate espionage, improved identification of user-preferences, distributed product testing	Tool for employee vetting, intelligence source for counter-terrorism, tool for foreign espionage, novel means to monitor citizen behaviour
ORGANISATIONAL CAPABILITIES	Global reach, issue-specific crowd-sourcing, rallying tool, e.g., for subversive purposes	Global reach, issue-specific crowd-sourcing, e.g., for product improvement efforts (business) or activism (NGO)	Global reach, issue-specific crowd-sourcing, e.g., for supporting and steering (foreign) individuals, organisations and governments

Table 2. OVERVIEW OF THE SECURITY IMPLICATIONS OF SOCIAL NETWORKING

However, any consolidated assessment of the significance of social networks for security matters in the twenty first century would be premature, given the infancy of the phenomenon. This infancy is also evidenced by the relatively small body of literature on the subject which across the board, underlines the degree of uncertainty surrounding this phenomenon. Still, a number of additional insights may be distilled from the key findings in the foresight community.

Mobilising people using social networks is highly likely to increase in the future. Social networks are gradually getting more attention for their opportunities, risks and effective utilisation. Whereas social networks often function as an independent and uncensored medium in the Third World, the Obama campaign illustrates that social networks also mobilise people in the First World. In addition, the DARPA contest indicates that the organising potential of social networks go beyond just the political domain. Although the foresight community previously neglected the effects of social networks in First World countries or beyond the political domain, there is now a shift towards getting a more complete understanding of the effects of social networks. Reports now also look at (1) social networks as a novel method for strategic communication, (2) opportunities in social networks for governments, (3) identifying new and useful domains for the application of social networks in communication (such as in public services) and (4) understanding the scope and impact of social networks in general.

Beyond specific computing issues such as malware and data defence, the impact of social networks on state and organisation security is only recently starting to receive attention. This development indicates that social networks are becoming a part of everyday life and that governments and non-governmental organisations are starting to appreciate that information security is vital in this information age. This also means that the contribution of social networks as a strategic security issue is growing because of the new vulnerabilities, such as corporate espionage, that social networks introduce. Now that public and private actors alike have experienced their first security breaches through social networks, the role of these social media will likely receive more attention in the years to come.

Social networks represent not just a threat to security, they also offer numerous advantages such as improved information dissemination or novel organisational practices. However, so far there has been very little attention dedicated to the

ways in which states can leverage the benefits of social networking. Most studies approach social networks at a technical level or as security threats but not as much as potentially powerful communication and governance tools. Moreover, even within this approach, social networking is addressed at the operational level rather than at the strategic level, often achieving and noting tactical and incident-specific successes only such as CAVNET for monitoring Iraqi insurgents, as opposed to understanding social networks' impact on public opinion or on information warfare as a whole.[30]

Social networks will provide a platform to a broader spectrum of voices that may alter the status of 'expert opinion' in the public debate. They may enhance the staying power of citizens and consumers vis-á-vis governmental authorities and corporations; conversely, they may also strengthen the hand of regimes and corporations worldwide. In any case, social networks will affect the ability of government and corporations to shape their environment.

As social networking continues to spread, governments and corporations will have to devise strategies in order to cope with the strategic impact of social networks on government and corporate communication, information security, information dissemination, intelligence operations, and organisational capabilities.

Annex I: Operationalisation of parameters

Parameters

Social network organisation
This parameter refers to a future where social networks are dominated by a single great network or instead by numerous distinct, niche social networks. Scaling: central/medium/niche

Ubiquity of social networking
This parameter involves the penetration of social networks in society, namely the amount and type of technology that is available to a social network user. Scaling: low/med/high

Quality of the information
This parameter refers to the quality of the information on social networks. Is it real, fake or even relevant? Scaling: low/med/high

Technical architecture
This parameter describes the technical back-end or architecture of the social network itself. Scaling: centralised/med/decentralised

Trust
This parameter measures the trust people have in a social network and their willingness to use it for sharing information. Scaling: low/med/high

Security defences
This relates to the security of the social network. Is the future of social networking more secure or are the risks of security breaches high? Where are the defences: are they server-side or client side? Scaling: user/med/server

Drivers

Accessibility
This driver relates to the accessibility of social networks to users. The driver can be broken into a number of sub-factors such as user-friendliness with a friendly user-interface as well as technical accessibility, e.g. by having social networks on mobile phones.

Benefits
This driver refers to the benefits a user derives from participating in a social network. Examples of benefits include the availability of services, the number of friends, etc.

User data availability
This involves the availability of real-life user data on a social network. For example, LinkedIn has real user data on its network, not fake profiles.

Security
This driver encompasses security issues with social networks in its broadest sense. Examples of security issues are user data security issues or network security issues.

Privacy
This driver encompasses broad privacy issues with social networks.

Trust
This driver refers to trust as an incentive to increase the use of social networks. The more people trust the network, the more it will be used.

Bandwidth
This driver relates to the amount of bandwidth available for social networks.

Security Implications

Information security
This refers to the information security of data on a data, personal and organisational level.

Organisational capabilities
Social networks impact the way people organise. This can be on operational, tactical and strategic levels.

Intelligence operations
There are increased opportunities to collect intelligence on social networks.

Information dissemination
Information dissemination describes the ability of users to disseminate information through social networks on an individual, corporate and governmental level.

Endnotes

1 J.J. Carafano, "All a Twitter: How Social Networking Shaped Iran's Election Protests" (Heritage Foundation, 2009), http://www.heritage.org/research/internetandtechnology/bg2300.cfm.

2 B. Stone and N. Cohen, "Social Networks Spread Defiance Online", *The New York Times*, June 15, 2009, http://www.nytimes.com/2009/06/16/world/middleeast/16media.html?_r=1.

3 See the Facebook website "Company Timeline", http://www.facebook.com/press/info.php?timeline (accessed 14 December 2009).

4 Sam Jones and Richard Norton-Taylor, "'Congrats to Uncle C' – how his wife's Facebook page exposed new MI6 head", *The Guardian*, July 5, 2009, http://www.guardian.co.uk/politics/2009/jul/05/mi6-facebook-sawers-wife-miliband.

5 See the Profilactic website: http://www.profilactic.com/, (accessed 6 January 2010).

6 Help Net Security, "19% of online attacks in 2009 targeted social networking sites", http://www.net-security.org/secworld.php?id=7882.

7 ENISA, "Web 2.0 Security and Privacy", 2008, 28, http://www.enisa.europa.eu/act/it/oar/web-2.0-security-and-privacy/web-2.0-security-and-privacy.

8 V. Seppa, "The Future of Social Networking", in , 2008, 3, http://www.cse.tkk.fi/en/publications/B/1/papers/Seppa_final.pdf.

9 J. Menn, "ID thieves find a niche in online social networks", *LA Times*, May 5, 2008, http://articles.latimes.com/2008/may/05/business/fi-socialid5.

10 D. Rand, *Threats when using Online Social Networks* (CSIS Security Research and Intelligence, 2007), http://www.csis.dk/dk/forside/LinkedIn.pdf.

11 B. Collins, "Microsoft leaks details of Windows 8 and Windows 9", *PC Pro*, October 8, 2009, http://www.pcpro.co.uk/news/enterprise/352270/microsoft-leaks-details-of-windows-8-and-windows-9.

12 S. de Jong, "Cursus hyven voor Defensiepersoneel", *NRC Next*, April 2009, http://www.nrcnext.nl/geld-en-werk/2009/04/13/cursus-hyven-voor-defensiepersoneel/.

13 ScanSafe, *Social Networking – What Every Business Should Know (A ScanSafe Whitepaper)* (ScanSafe, 2008), 6, http://www.scansafe.com/whitepapers.

14 ENISA, "Online Social Networks", 2007, 12-13, http://www.enisa.europa.eu/act/it/library/pp/soc-net.

15 In their report, M. Drapeau and L. Wells, "Social Software and National Security: An Initial Assessment" (Center for Technology and National Security Policy National Defense University, 2009), http://www.ndu.edu/ctnsp/Def_Tech/DTP61_SocialSoftwareandNationalSecurity.pdf., government functions are analysed but these streams are applicable to organisations in general too.

16 Maj. Patrick Michaelis, "Innovating & Improvising", http://www.pbs.org/wgbh/pages/frontline/shows/company/lessons/.

17 Drapeau and Wells, "Social Software and National Security: An Initial Assessment", 10-12.

18 N. Anderson, "Israel/Hamas battle goes Web 2.0", *Ars Technica*, 2009, http://arstechnica.com/web/news/2009/01/israelhamas-battle-goes-web-2-0.ars.

19 Elliot Schrage, "New Media Tools and Public Diplomacy", 2009, http://www.cfr.org/publication/19300/new_media_tools_and_public_diplomacy.html; Congressional Research Service, *Social Networking and Constituent Communication: Member Use of Twitter During a Two-Week Period in the 111th Congress*, 2009, http://assets.opencrs.com/rpts/R40823_20090921.pdf.

20 The Huffington Post, "Palin: Obama's "Death Panel" Could Kill My Down Syndrome Baby", http://www.huffingtonpost.com/2009/08/07/palin-obamas-death-panel_n_254399.html; SEROXAT SUFFERERS - STAND UP AND BE COUNTED, "HPV Vaccine Video on Youtube", http://fiddaman.blogspot.com/2009/03/acdc-what-band.html.

21 K. Wheaton, "Top 5 Intelligence Analysis Methods: Social Network Analysis (#3)", *Sources and Methods*, December 11, 2008, http://sourcesandmethods.blogspot.com/2008/12/top-5-intelligence-analysis-methods_11.html.

22 Silva et al., "Virtual Forensics: Social Networking Security Solutions", *Proceedings of Student-Faculty Research Day, CSIS, Pace University* (2009): 2, http://csis.pace.edu/~ctappert/srd2009/a3.pdf.

23 J. Wortham, "More Employers Use Social Networks to Check Out Applicants, *New York Times Bits*", August 20, 2009, http://bits.blogs.nytimes.com/2009/08/20/more-employers-use-social-networks-to-check-out-applicants/.

24 CyberSecurity Malaysia, *Cyber Security Incident Outside Malaysia* (Ministry of Science, Technology & Innovation, 2008), 5.

25 J. Vargas, "Barack Obama, Social Networking King", *The Washington Post, The Trail*, October 6, 2007, http://blog.washingtonpost.com/44/2007/10/06/barack_obama_social_networking.html.

26 J.J. Carafano, "Social Networking and National Security: How to Harness Web 2.0 to Protect the Country" (Heritage Foundation, 2009), 1, http://www.heritage.org/Research/NationalSecurity/bg2273.cfm.

27 Drapeau and Wells, "Social Software and National Security: An Initial Assessment", 20.

28 Ibid., 21-22.

29. M. Hesse, "Spy vs. spy on Facebook", *The Washington Post*, December 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/12/06/AR2009120602558.html.

30. Although this type of understanding is emerging and not entirely neglected either, for example, see: C. Dauber, "YouTube War: Fighting in a World of Cameras in Every Cell Phone and Photoshop on Every Computer", 2009, http://www.strategicstudiesinstitute.army.mil/Pubs/display.cfm?pubID=951.

In recent years, social networking sites have emerged as immensely popular Web 2.0 applications. Their ability to influence major events was demonstrated in the 2008 U.S. presidential elections and the 2009 post-election turmoil in Iran. These events have shown that social networks enable civic engagement and the quick mobilization of resources, as well as the uncensored spread of information. At the same time, new levels of information sharing have also left individuals, organisations and even governments vulnerable to a loss of privacy, data theft and espionage.

For better or worse, the emergence of social networks has profound implications in the realm of security. This FUTURE ISSUE reviews the nascent debate on this new phenomenon within the foresight community. Although any consolidated assessment of the significance of social networking for security in the twenty-first century would, given its infancy, be premature, this report highlights the most prominent drivers of this emerging trend, and suggests security implications for the future.

As social networking continues to spread, governments and corporations will have to devise strategies in order to cope with the strategic impact of social networks on government and corporate communication, information security, information dissemination, intelligence operations, and organisational capabilities.

The Hague Centre
for Strategic Studies

Lange Voorhout 16
2514 EE The Hague
The Netherlands

info@hcss.nl
www.hcss.nl