Information operations on the Internet

A catalog of modi operandi

ULRIK FRANKE

FOI-R--3658--SE
ISSN 1650-1942
March 2013

Ulrik Franke

Information operations on the Internet

A catalog of modi operandi

Bild/Cover: FOI

Titel	Informationsoperationer på internet – En katalog över modi operandi
Title	Information operations on the Internet – A catalog of modi operandi
Rapportnr/Report no	FOI-R--3658--SE
Månad/Month	Mars/March
Utgivningsår/Year	2013
Antal sidor/Pages	33 p
ISSN	1650-1942
Kund/Customer	
FoT område	
Forskningsområde	
Projektnr/Project no	I35404
Godkänd av/Approved by	Lars Höstbeck
Ansvarig avdelning	Informations- och aerosystem

Sammanfattning

Modern informations- och kommunikationsteknik erbjuder nya sätt att målsöka och påverka den allmänna opinionen. Sociala nätverk som Facebook, mikrobloggar som Twitter, videotjänster som YouTube och sökmotorer som Google möjliggör var och en sina sätt att styra hur utvalda individer uppfattar informationsmiljön. Därmed påverkas deras vilja, förståelse och förmåga.

Den här rapporten innehåller en katalog av internetbaserade tekniker för informationsoperationer, baserad på en genomgång av vetenskaplig litteratur, nyhetsrapportering och offentliga upphandlingar. Teknikerna är kategoriserade enligt svensk och Nato-doktrin för informationsoperationer. Målsättningen är inte att diskutera tekniska detaljer, utan att informera beslutsfattare om de nya möjligheterna för en motståndare att styra informationsmiljön. Även om många aktörer kan använda internet i propagandasyfte fokuserar rapporten på de modi operandi som är tillgängliga för statsaktörer.

Utöver själva katalogen identifierar rapporten även några strategiska implikationer av informationsoperationer på internet, såsom utökad räckvidd, oavsiktliga konsekvenser, problem i militär operativ planering och möjligheterna att vilseleda automatiska verktyg för så kallad *buzz monitoring*.

Nyckelord: Internet, informationsoperationer, psykologiska operationer, propaganda, falska gräsrotskampanjer, internet-strumpdockor

Abstract

The advent of modern ICT offers new means by which to target and influence public opinion. Social networks like Facebook, microblogs like Twitter, video services like YouTube and search engines like Google all offer particular means to shape the information environment as perceived by targeted sets of individuals, thus influencing their will, affecting their understanding and impacting their capabilities.

This report offers a catalog of available Internet techniques for information operations based on a review of scientific literature, media reporting, and government tenders. The techniques are categorized according to Swedish and NATO information operations doctrine. The aim is not to discuss the technical aspects in detail, but rather to inform policy makers of the new possibilities for adversarial shaping of the information environment. While many actors can use the Internet for propaganda, the focus of the report is on modi operandi available to state actors.

Apart from the catalog itself, the report also identifies some strategic implications of information operations on the Internet, including increased range, unintended consequences, the difficulties of military operational planning and the prospects for deception of automated buzz monitoring tools.

Keywords: Internet, information operations, psychological operations, propaganda, astroturfing, sock puppetry

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 has benefitted from the comments of many people. In particular, Fredrik Konnander from the Swedish National Defence College offered insightful and detailed comments that substantially improved the manuscript when he acted as the opponent at a research seminar. Jerker Hellström, David Lindahl and Steven Savage also gave valuable input at the seminar.

Stockholm, March 2013
Ulrik Franke, SPIS project manager

Table of contents

1 Introduction

The advent of the information society has changed the world. We now routinely work, play, buy things, educate ourselves and socialize with each other in ways not conceivable twenty years ago. The Internet is a digital infrastructure that is becoming as important to society as electricity, roads and water supply.

The sheer size of our collective endeavors is impressive. Wikipedia contains more than 4 million articles as of January 2013 [55], Facebook has one billion monthly active users as of October 2012 [15], and Twitter sports half a billion tweets a day as of October 2012 [53]. A key driver behind these numbers is the evolution from web 1.0, where publishers created material and made it available to an audience, to web 2.0, where user-generated contents has blurred the line between producers and consumers [26].

But this brave new world of abundant digital information is not without perils. In January 2013, shortly before the World Economic Forum, its organizers released a *Global Risks Report*. One chapter is dedicated to the global risk of "massive digital misinformation". It begins with the cautionary tale of how tens of thousands of Americans in 1938 confused a radio adaptation of the HG Wells novel *War of the Worlds* with the real thing – an invasion from Mars. Back then, the radio was a young medium, the power of which was not fully understood – somewhat akin to the Internet of today [14].

However, the most sinister aspect of massive digital misinformation is that it is not limited to accidents. On the contrary, willful deception on the Internet is very real. Social networks like Facebook, microblogs like Twitter, video services like YouTube and search engines like Google all offer distinctive ways to shape the information environment as it is perceived by targeted sets of individuals. Information from the Internet is often uncritically absorbed without detailed knowledge of its origins or reliability. Furthermore, precise targeting of specific individuals has never been easier than in today's information society: information that used to require days or weeks of surveillance can now be harvested in a few minutes from social networks online. Martin C. Libicki has coined the term "retail conquest in cyberspace" for this phenomenon [31], and Evgeny Morozov has polemically explained "why the KGB wants you to join Facebook" [36]. Even if the information thus obtained can be noisy and biased by everyone's wishful self-projections onto social networks, it still offers an avenue to influence. Psychologists at the University of Cambridge have shown that sensitive attributes such as homosexuality, religion, political party membership and use of cigarettes, alcohol, and drugs can be predicted with surprising accuracy from Facebook "likes" [47].

The fact that the Internet is used as a vehicle for psychological operations is not new. However, to date, there has been no systematic compilation in the literature of the modi operandi available to the would-be Internet propagandist. This report aims to rectify this, offering a catalog of available Internet propaganda techniques based on a thorough review of scientific literature, media reporting, and government tenders. The techniques are categorized using Swedish and NATO information operations terminology. The aim is not to discuss the technical aspects in detail, but rather to succinctly inform about the possibilities for adversarial shaping of the information environment. While many actors can use the Internet for propaganda, the focus of this report is modi operandi available to state actors.

1.1 Scope

This report is primarily about how state-actors can conduct information operations on the Internet. Private citizens' social networking, corporations' marketing, and political parties' campaigning are thus out of scope for this report, though they have served as inspiration in cases where there is overlap with what state-actors can do.

This report is primarily about online action. Governments often supplement online practices such as filtering and blocking with offline practices designed to deter users from publishing certain contents. These measures include legal prosecution, imprisonment, physical attacks, or other forms of harassment [27]. Such offline action is thus considered out of scope, unless conducted in close concert with online action.

1.2 Outline

The remainder of the report unfolds as follows. In Section 2, a brief background on censorship and influence is given. Section 3 contains the main contribution, i.e. the catalog itself. Section 4 discusses some strategic implications, and Section 5 concludes the report.

2 Censorship and influence

As this report has a focus on state actors, it is necessary to discuss censorship and its relationship to more subtle influence. Cunningham & Wasserstrom, in their analysis of China, point out that even though censorship (blocking, filtering and taking websites offline) receives a lot of attention, this is just one side of the coin. The flip side is a charm offense that they dub Control 2.0 [10]. This distinction is similar to the old *hard power* (akin to censorship) vs. *soft power* (akin to influence or propaganda) distinction in traditional security and international relations studies.

Deibert & Rohozinski from the *Open Net Initiative* offer a good intellectual framework for understanding and reasoning about these issues. They distinguish three generations of Internet control [12]:

1. First generation: Filtering and blocking (servers, domains, IP addresses, key words).

2. Second generation: The creation of a legal and normative environment where government can selectively deny the public access to information on the Internet if and when it is ‘needed’. The *overt* part of this consists of laws that regulate ‘acceptable’ contents, and laws against libel and slander. The *covert* part consists of putting pressure on ISPs and using distributed Denial-of-Service (DDoS) attacks to take out sites.

3. Third generation: The aim is not to *deny* access to information, but rather to *compete* for attention, and hide criticism in a flood of other contents. These actions can be guided by sophisticated methods such as Internet surveillance and data mining, and be carefully targeted to demoralize and discredit opponents.

It should be emphasized that the generations are not necessarily distinct. Deibert & Rohozinski, based on their case-studies of the post-Soviet states, conclude that the most authoritarian states appear to be using all of the generations at the same time, whereas the hybrid regimes and flawed democracies stick to the second and third generations.

If the military school of thought on information operations [39] is applied to the generations of Internet control, another feature appears: first generation control is mostly about affecting the *capability* of the opponent, whereas second and third generation are mostly about affecting his *will* and *understanding*. This distinction is important, since methods affecting capability are typically perceived as being more coercive (filtering and blocking) or even violent (seizing servers) than the methods that affect will and understanding (persuasion, threatening or just framing an issue away). If a state actor shifts modus operandi from first to second and third generation methods of control, this will probably be perceived as more lenient and less controversial, though the *effects* achieved remain the same.

As will be evident in the next section, elements from all of the generations can be used to conduct information operations through the Internet. This is no surprise. For example, NATO information operations doctrine points out that “Info Ops is an integrating function focused on the information environment that involves the selective combination of lethal and non-lethal means to achieve campaign objectives” [39]. This “selective combination” applies on the Internet as well. When reading the catalog, it is important to consider how each modus can be exploited in concert with the others, in order to reach the overall desired effect.

3 Catalog

The catalog is structured according to the Swedish Armed Forces taxonomy of information operation *tasks* [18], each of which is defined in accordance with NATO doctrine [39]. This taxonomy is not perfect. For example, some (aspects) of the tasks exhibit overlap, meaning that not every modus can be unambiguously placed. Furthermore, some of the wordings (e.g. the “coalition” term) are not really applicable outside of the NATO context. Nevertheless, the structure and rigor provided by the taxonomy is valuable.

By its very nature, the catalog deals with sensitive and covert issues. Although all efforts have been made to ascertain that the examples given are accurate, they should be read with a critical mind. When in doubt, the sources cited should be scrutinized and assessed. More important, however, is that the modi described are feasible *in principle*. Even if it should turn out that they have not been employed precisely as described, they do contribute to spanning the feasible action space.

3.1 Diminish

Definition: To make less or cause less to appear. To reduce the effectiveness of an activity. (This is similar to degrade, without the lethal overtones.) [*39*]

- A traditional way to diminish the impact of information that threatens one’s interests is to spread denials and denigrations through the web. Chase & Mulvenon describe the Chinese strategy of propaganda websites such as the now defunct humanrightschina.org that advanced the official government line that there are no human rights abuses in the country [6].

- A more modern way is the use of social media to diminish the magnitude of events. The number of participants in protests is a typical subject. For example, on 7 August 2012, Russian opposition leader Aleksey Navalny was asked on Twitter “how many crouched with [him] back then on the [Bolshoy] Kamenny [Brigde]? One or two hundred?”,[1] taunting the opposition ‘March of Millions’ by diminishing the number of participants.

[1] The full tweet read: “@navalny @romanvolobuev Слабоумия и отваги. Миллион и зимой не вышел. А сколько вокруг тебя присело тогда на Каменном? Сто, двести?”

3.2 Expose

Definition: To make known or cause to be visible to the public eye. To make visible, to reveal something undesirable or injurious. [*39*]

- Exposure does not need to be accurate to spread and have an effect. False or manipulated images can be spread on the Internet, e.g. by taking weapons from soldiers killed in action and rearranging their bodies to make them look like massacred civilians [9].

- Following the Russian duma election in December 2011, email exchanges and other private correspondence (illegally collected) was 'leaked' to the press in order to discredit opposition leaders [13].

3.3 Influence

Definition: To cause a change in the character, thought, or action of a particular entity. (Selected projection or distortion of the truth to persuade the opposition to act in a manner detrimental to their mission accomplishment while benefiting accomplishment of friendly objectives.) [*39*]

- Various ways to prevent access to Internet material will be recurring throughout the catalog, but in the context of influence, it is worth making the general point that filtering out some opinions will give other opinions a head start [54].

- Unsophisticated propaganda might be effective: if not to sway opponents, then to encourage followers. The Assad regime in Syria, or its supporters, is spreading Youtube-movies where the Al Jazeera logo is destroyed [17].

- Distributing messages with an ambiguous (grey) or outright false (black) source is a way to influence opinions. Allegedly, Pentagon contractors wrote pro-Western stories for Iraqi newspapers in 2004-2005 [54], and websites on African or Balkan politics have been run by the US military [5]. ”Cloaked websites” have been systematically studied in the white supremacist context, where concealed authorship was identified as a way to make propaganda more effective [11].

- However, the advent of social media offers new routes to influence. Early examples involve chat rooms and instant messaging services: the US Defense Science Board noted that the Bush and Gore campaigns of 2000 used methods similar to the Chinese government for conducting "guided discussion" designed to influence citizens [34]. Today, North Korea uses social networks to spread its propaganda [45]. The potential for grey or black influence operations on social networks is huge, as Facebook is estimated to have about 83 million fake users [52], and 'likes' can readily be manipulated or bought [50].

- When influence activities such as these are coordinated on a larger scale, they can give the false impression that a large grass-root movement is behind a certain opinion. This phenomenon – dubbed astroturfing – has received a lot of attention. Ratkiewicz et al.[2] have written about how to detect Twitter-astroturfing [44]. They list the following common techniques for increasing the impact of tweets [44]: (i) Have a single person control two different accounts, to give the impression that several people are tweeting on the same topic. (ii) Use exclusive accounts dedicated to retweet some messages. (iii) Establish a web page and use a bot net with several Twitter accounts to post links to it. Add different hashtags and scramble links with dummy parameters so that they are not identical and thus easily detectable. (iv) Use bots to approach popular users in a coordinated way, so that they perceive a message as coming from several different sources, deem it credible, and retweet it.

- Influencing through social networks can also be achieved using fake users on a larger scale – so called *sock puppetry*. In March 2011, a US federal contract with Ntrepid was exposed by the Guardian, revealing blueprints for a technical system allowing an operator to control the actions of ten fake social network personas supplied with credible backgrounds, using VPN solutions to avoid detection [16] [1]. In a remarkably similar turn of events, Russian daily Kommersant exposed a tender from the Foreign Intelligence Service SVR concerning a system built for "massive dissemination of information messages in designated social networks with the purpose of forming public opinion" [4]. The

[2] Cf. also http://truthy.indiana.edu/

operation of the envisioned system seems close to its American counterpart.

3.4 Inform

Definition: To impart information or knowledge. [*39*]

- Information can be imparted through dedicated websites, as suggested by Brigadier General Sapan Kumar Chatterji for the purpose of countering terrorism [7].
- Twitter is another vector, as employed by e.g. the US State department [32].
- Using ‘new media’ including Facebook, Twitter etc. to improve government emergency communication e.g. in the event of natural disasters is an established research area [3].
- YouTube is another vector for government information, used for example by the US Office of National Drug Control Policy (ONDCP), which released eight commercials on drug control in September 2006 [22].
- The Chinese State Council Information Office offers an iPad app with recorded press conferences and white papers on various subjects [10].
- In many countries, governments are adopting “open data” strategies to foster transparency, efficiency and innovation by making large public datasets available online [23].

3.5 Prevent

Definition: To deprive of hope or power of acting or succeeding. To keep from happening, to avert. [*39*]

- Governments (particularly authoritarian ones) have a number of tools at their disposal for imposing what Freedom House calls *obstacles to access* [27], including “infrastructural and economic barriers to access; governmental efforts to block specific applications or technologies; and legal, regulatory and ownership control over internet and mobile phone access providers". These will not be discussed at length here.

- The use of (i) hacking or (ii) distributed Denial-of-Service (DDOS) attacks (which are less sophisticated) to attack opponent web sites is a more operational measure. Chinese authorities have probably attacked Falun Gong sites [6] and human rights groups at home and abroad [27] in this way. Such attacks are hard to attribute, entailing deniability.

- Another modus, known from Belarus, is to slow down Internet connections (by order or by attack) to the point of making them useless, while retaining deniability and being able to blame technical performance problems [27] [45].

- User-feedback where content is reported as offensive can be used to get rid of unwanted material. This has been known to work on Facebook and YouTube, and examples abound (e.g. China, Egypt, Ethiopia, Mexico, and Tunisia) [27]. A variation of the user feedback mechanism is to report the target website as being infected by malware to databases such as Google's. If this is systematically done by many users (e.g. through bot nets), the site will be blocked or removed from search results.

- An alternative approach for preventing a target audience from using the Internet in a meaningful way is to infiltrate mailing lists, forums and discussion groups. The Chinese government has allegedly used vulnerabilities in mail protocols to send false e-mails between dissidents, spreading disinformation and creating strife among groups. Discussions about who is actually an infiltrator hired by Beijing are common on such forums – preventing useful coordination and leading to the speculation that these discussions as such are actually initiated by Chinese special services [6]. The same strategy is said to be employed by the US State Department to counter would-be-terrorists by 'trolling' their forums on the Internet. The concept is called *Viral Peace* and aims to disrupt the narcissist and self-righteous environment needed for radicalization on Internet forums [2].

3.6 Protect, Safeguard

Definition: To cover or shield from exposure, damage, or destruction. To keep from harm, attack, injury or exploitation. To maintain the status or integrity of. To take action to guard against espionage or capture of sensitive equipment and information. [*39*]

- A way for a government to maintain a status quo of information superiority is to crowd out alternative voices by increasing the level of noise. The infamous Chinese ‘50-cent party’ – tasked with flooding the Internet with pro-government commentary – are said to number 40 000 [45].

- Assad loyalists apply a similar flooding tactic, filling rebel Facebook-walls with denigrating comments and using bots to flood the Twitter hashtag #Syria with irrelevant information to crowd the opposition out [45] [43].

3.7 Negate, Neutralize

Definition: To render ineffective, invalid or unable to perform a particular task or function. To counteract the activity or effect of. [*39*]

- Governments around the world have become infamous for imposing what Freedom House calls *limits on content* [27], e.g. filtering and blocking of websites, other forms of censorship including self-censorship, and content manipulation. A straightforward example is the South Korean block of North Korean websites including the official North Korean Twitter account [27]. Such content control can take place on four different levels: the Internet backbone, the Internet service provider, the institutional level (universities, government agencies, schools etc.) and the end-user computer by means of filtering programs [40]. On the higher levels, the cruder strategy is to block IP addresses or URLs. Keyword blocking, which requires the contents of the traffic to be continuously processed, is more sophisticated. On the level of the end-user, the Chinese keyword filtering regime is built into instant messaging systems such as TOM Skype and QQ [27]. Deep packet inspection (DPI) technology represents a new step in Internet control, where not only the ‘headers’ of data packets (i.e. addressing information) are inspected, but also the actual contents. The intrusive nature of DPI has made it a sensitive issue in Russia, where recent legislation seems to mandate its use on the ISP level [51].

- An offline way to counter criticism in the blogosphere is by print media: on Cuba, government newspapers smear oppositional bloggers [45].

- Unwanted opinions can also be countered on the Internet. An institution like the Chinese 50-cent party can be used not only as the noise-generator described above, but also as online bullies, harassing those expressing unwanted opinions. Thus, Thailand uses the military to counter criticism of the monarchy on the Internet, and the existence of Russian “web brigades” under the control of the FSB is a persistent rumor, though difficult to prove [27].

- Opposition can also be passively engaged. For example, the Chinese Academy of Social Sciences maintains an anti-Falun Gong website that draws on the CASS scientific credibility [6].

- Hacking is a more active measure for neutralizing unwanted contents. Thus Syrian pro-Assad hackers took over a blog and Twitter account belonging to Reuters and used it to spread false (and sometimes absurd) information [8].

- A few more sophisticated ways for authoritarian states to neutralize online dissent are proposed by Morozov [35]: (i) Critical bloggers who have exposed local corruption can simply be bought by the authorities and become figureheads for meaningless state sanctioned information campaigns. (ii) By creating forums and mechanisms for listening to the people, dissent can be managed. The forums and mechanisms can then simply be ignored. (iii) The Russian case shows that it is possible for the government to support websites with superficial political contents, that quickly morphs into apolitical entertainment: Morozov observes that “[t]he Russian authorities may be on to something here: The most effective system of internet control is not the one that has the most sophisticated and draconian censorship, but the one that has no need for censorship whatsoever.” Lipman and Petrov make the similar observation that the Internet offers an opportunity to ‘let off steam’ without it necessarily having any consequences in the offline world [33].

3.8 Shape

Definition: To determine or direct the course of events. To modify behavior by rewarding changes that lend toward a desired response. To cause to conform to a particular form or pattern. [*39*]

- One important way to shape perceptions (and thus behavior) is to manipulate search results [40]. China is the token example, where search-engine providers are forced to adjust search results to match the criteria of those in power [27]. A more crude way to stop searches for certain topics is filtering based on words in the URL [56].

- In light of the previous modus, it might be thought that governments (at least authoritarian ones) do not need to bother with more mundane search engine optimization (SEO). This is not the case. Chinese scholars research and publish strategies for how to improve the rankings of government websites on search engines, exploring the impact of keywords, hyperlinks etc. [25] [30]. Similarly, on the official Russian website for government tenders, a considerable number of contracts for search engine optimization are readily found.[3]

- A similar way to shape people's knowledge is strategic Wikipedia editing – a strategy available to everyone, including governments. Famous examples include the US [41] and Australian [37] governments. At least one website has been created to monitor the IP addresses of Wikipedia editors, in order to expose such cases.[4]

- A more direct way to shape action is timely web forgery connected to particular events. The Belarusian authorities have applied this tactic, providing incorrect locations for opposition rallies on nearly identical clones of legitimate websites to which users were redirected by the state owned Belpak ISP [27].

[3] A Google search for "Поисковая оптимизация" site:zakupki.gov.ru rendered more than 100 results in January 2013.

[4] Cf. http://wikiscanner.virgil.gr/

3.9 Detect

Definition: To discover or discern the existence, presence, or fact of an intrusion into information systems. [*39*]

- Phishing for usernames and passwords to social media has been reported from Syria and Iran, as have more sophisticated methods involving forged SSL certificates [45]. Tunisian security officials under the Ben Ali regime regularly broke into e-mail and social media accounts of opposition activists [27]. China is known to use a potent combination of phishing and malware to keep track of the Tibetan opposition [38]. Since June 2012, Google notifies users of Gmail and Chrome if they "believe state-sponsored attackers may be attempting to compromise your account or computer" [42]. To some extent, this levels the playing field between state-actors and individuals, but such warnings also create incentives for new stealthier methods. It also opens the possibility to *deliberately* trigger the Google alarm in order to deliver a message.

3.10 Deter

Definition: To turn aside, discourage, or prevent a potential or actual adversary or other target audience from taking actions that threaten coalition interests. [*39*]

- E-mails to key individuals can be used to deter or discourage certain actions, a modus employed by both sides in the Kosovo war of 1999 [34] and by the US against Iraqi officials in the prelude to the war in 2003 [49]. In the 2012 conflict between Israel and Hamas, the IDF used Twitter in a similar manner to deliver messages both to Hamas leaders [28] and to journalists [20].

- Incentives for self-censorship can be created by making owners of servers or websites legally responsible for all contents, including that written by others. Such practices have lead Chinese Internet companies to hire several hundreds of thousands of censors to continuously monitor blog posts, comments, videos etc. [27]. In Russia, the Civil and Penal Codes have been used to curb unwanted contents on the Internet, not least the federal law 'On Counteracting Extremist Activity' [46]. US government agencies have put pressure on ISPs to 'voluntarily' shut down websites in order to stop terrorist financing [24]. It should be stressed that this modus is not only used to get rid of unwanted material *ex post*, but to incite self-censorship *ex ante*. The *Open Net Initiative* notes that this can be achieved by spreading the belief (more or less true) that the government monitors the Internet [40].

- Outsourcing censorship to private contractors or entities is becoming increasingly common, in China but also elsewhere [29] [45]. This modus can entail greater deniability from government agencies, and also make the censoring practices less transparent.

3.11 Promote

Definition: To contribute to the progress or growth of; further. [*39*]

- Electronic media can be employed to promote policy. Faced with anti-Japanese rallies in April 2005, the Chinese government sent text messages to all customers within the China Mobile network, reassuring the recipients that the government was managing foreign policy in the most beneficial way [29].

- *Ideotainment* is a term coined by Lagerkvist to describe Chinese efforts to make the official ideology ‘cool’ in the eyes of the next generation [29]. It uses “intermeshing of high-tech images, designs, and sounds of popular Web and mobile phone culture with subtle ideological constructs, symbols, and nationalistically inclined messages of persuasion”. The measures taken to censor the Internet are always described with wordings like ”youth”, ”health”, ”hygiene” and ”pollution” [29].

- A more traditional way to manage the information environment and promote the desired themes and messages is government-run news agencies. Following the 1999 bombing of the Chinese embassy in Belgrade, party mouthpiece People's Daily set up a “Strong Country Forum” website, a nationalist forum that turned out to be popular. A year later a million RMB[5] was used to create five new information and news agencies, each with carefully designed websites [29].

- Lagerkvist, describing the Chinese situation, identifies three methods for regime promotion mixing information and propaganda, viz. (i) e-government-projects, (ii) state-owned and municipal news portals and (iii) information campaigns [29].

- One modus that can be used in an environment normally rigorously censored is to suddenly lift censorship in order to promote a certain topic. Vietnam, which usually runs a strict censorship regime, in June 2011 allowed anti-Chinese sentiments on Facebook, and Internet-coordinated anti-Chinese rallies [17]. Failure to censor is, in this context, also a kind of promotion.

[5] The *renminbi* is the currency of the People's Republic of China.

4 Strategic implications

Deibert & Rohozinski introduced their three generations of Internet control taxonomy in order to explain the fact that traditional filtering and censorship is rarer in the Russian-speaking part of the Internet than one would expect, given the grim state of political freedom in most post-Soviet countries. But they also offer good arguments to believe that second and third generation Internet control is likely to become more common throughout all of the Internet [12]. If this line of reasoning is correct, then it also implies an *increased range* for Internet influence operations. Modi that depend upon physical control of servers and infrastructure can only be carried out on one's own territory. Modi that hinge upon norms and legislation might reach a bit further, through diaspora and international agreements. But modi that compete for attention on the Internet can reach far beyond state borders and affect people all over the world.

Another implication has to do with *unintended consequences*. The fact that there are many powerful tools for Internet influence available does not mean that those who use them always achieve their intended purpose. In terms of first generation Internet control, the Mubarak regime in Egypt is a good example. It has been argued that the desperate attempt to regain control of the situation by disconnecting the country's Internet access actually provided an unintended rallying call to the opposition, accelerating the fall of the regime [21]. In terms of second and third generation modi, a plausible unintended consequence is a gradual loss of situation awareness, as it becomes more difficult to see what is genuine public sentiment, and what is prompted by one's own influence operations. Some suggest that China might now be experiencing this effect. If so, it is the digital equivalent of the German government's failed attempt in 2003 to ban the neo-Nazi NPD party, when the Federal Constitutional Court rejected the ban because paid informers from intelligence services might in part have shaped party policies [19]. Furthermore, Internet communities are very sensitive to exposed attempts to influence them. This means that information operations can backfire by provoking an intense and unintended response directed back towards the originator. While the one-way communication propagandist broadcasting radio never had to worry about the target audience broadcasting back, the two-way communication propagandist on Twitter always runs the risk of being exposed and ridiculed.

Military operational planning is also complicated by the fact that the importance of public opinion in modern conflicts is hard to over-estimate. From peace-support operations, through counter-insurgencies and asymmetric wars to full scale international armed conflicts, the perception of the public eye has become a battle ground just as real as the air, land and seas. But the full complexity of military information operations planning in the modern information society is so far unknown. While the November 2012 conflict between Israel and Hamas offers one of the first examples of a government attempting to fully synchronize kinetic action with real-time digital information operations, it also shows some of the difficulties. It has been pointed out that the Israeli messages simultaneously had to influence three different audiences – the enemy, the population of Israel, and the international community – and unlike printed leaflets, there was no easy way to keep them apart [48]. Furthermore, the campaign lasted only a few days, so the complexity of waging synchronized kinetic and information war for weeks, months or years remains unknown. The problems related to military planning clearly require further study, not least the key question of how to properly make the *tasks* given to military units actually contribute to the desired *effects* – and how to measure that contribution.

The issue of *attribution* – determining who is behind attacks – has been at the heart of cyber conflict discussions for a long time. With increasing threat awareness, methods and tools for detecting and attributing Internet influence operations (e.g. the *Truthy* project at the University of Indiana or the Google policy to warn targets of state-sponsored attacks) will surely become more commonplace. However, such tools themselves open the avenue to *second-order deception*, i.e. fooling the tools to offer a false attribution. The more documentation there is available on such tools, the easier they will be to target. Similar operations can be conducted against the evermore popular tools for buzz monitoring, i.e. tools that monitor and mine social media for information. If it is known that a certain organization is using a particular (commercial or open-source) buzz monitoring tool for its situational awareness about a certain topic, then an adversary can craft a deliberate deception attack, where knowledge of tool architecture and online sources offers a powerful route to influence. Intelligence organizations depending on the abundant open source information on the Internet will be particularly vulnerable.

5 Conclusions

The landscape of today's information society is complicated. While automation and user-generated contents create benefits, they also make us vulnerable to new kinds of influence operations. Information gathered online can be used for sophisticated target profiling. With the advent of second and third generation Internet control, government information operations are less constrained by state borders.

However, there is no going back to simpler times. In time, a "global digital ethos" [14] might evolve that makes the Internet more like radio, and all of us less susceptible to spread or believe in misinformation. Technical solutions like *Truthy*, that help users validate information found on the Internet, might aid us, and in time render certain psychological operations obsolete. But just like in any duel between measures and countermeasures, new modi will always surface. The task of updating the catalog presented in this report will never end.

6 References

[1] Spencer Ackerman. Jihadis’ Next Online Buddy Could Be a Soldier. http://www.wired.com/dangerroom/2011/03/jihadis-next-online-buddy-could-be-a-soldier/, March 2011. Wired, retrieved 18 January 2013.

[2] Spencer Ackerman. Newest U.S. Counterterrorism Strategy: Trolling. http://www.wired.com/dangerroom/2011/03/jihadis-next-online-buddy-could-be-a-soldier/, July 2012. Wired, retrieved 18 January 2013.

[3] Henrik Artman, Joel Brynielsson, Björn JE Johansson, and Jiri Trnka. Dialogical emergency management and strategic awareness in emergency communication. In *Proceedings of the 8th International ISCRAM Conference*, 2011.

[4] Ilya Barabanov, Ivan Safronov, and Elena Chernenko. Razvedka botom [Intelligence Using a Bot]. http://www.kommersant.ru/doc/2009256, August 2012. Kommersant, retrieved 7 November 2012.

[5] Adam Brookes. US plans to ’fight the net’ revealed. http://news.bbc.co.uk/2/hi/americas/4655196.stm, January 2006. BBC, retrieved 18 January 2013.

[6] M. Chase and J.C. Mulvenon. *You’ve got dissent!: Chinese dissident use of the Internet and Beijing’s counter-strategies*. Number 1543. Rand Corporation, 2002.

[7] S.K. Chatterji. An overview of information operations in the Indian army. *IO Sphere*, Special Edition 2008:10–14, 2008.

[8] Richard Chirgwin. Reuters suffers double hack. http://www.theregister.co.uk/2012/08/05/reuters_hacked/, August 2012. The Register, retrieved 18 January 2013.

[9] Deirdre Collings and Rafal Rohozinski. *Bullets and Blogs: New media and the warfighter*. United States Army War College, 2009.

[10] M.E. Cunningham and J.N. Wasserstrom. Authoritarianism: there’s an app for that. *Chinese Journal of Communication*, 5(1):43–48, 2012.

[11] J. Daniels. Cloaked websites: propaganda, cyber-racism and epistemology in the digital era. *New Media & Society*, 11(5):659–683, 2009.

[12] R. Deibert and R. Rohozinski. Control and subversion in Russian cyberspace. In Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, editors, *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, pages 15–34. MIT Press Cambridge, MA, 2010.

[13] Jonathan Earle. Youth Group Leader in Leak Scandal. http://www.themoscowtimes.com/news/article/youth-group-leader-in-leak-scandal/452277.html, February 2012. The Moscow Times, retrieved 8 February 2012.

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

[15] Key Facts – Facebook newsroom. http://newsroom.fb.com/content/default.aspx?NewsAreaId=22. Retrieved 19 January 2013.

[16] Nick Fielding and Ian Cobain. Revealed: US spy operation that manipulates social media. http://www.guardian.co.uk/technology/2011/mar/17/us-spy-operation-social-networks, March 2011. The Guardian, retrieved 18 January 2013.

[17] 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.

[18] *Handbok Informationsoperationer [Information Operations Handbook]*. Försvarsmakten [Swedish Armed Forces], Stockholm, 2008.

[19] Hubert Gude, Sven Röbel, and Holger Stark. The State vs. the NPD: High Hurdles for Possible Ban on Far-Right Party. http://www.spiegel.de/international/germany/legal-difficulties-in-possible-attempt-to-ban-npd-a-822327.html, March 2012. Der Spiegel, retrieved 20 January 2013.

[20] Daniel Halper. Israel Warns Journalists to Stay Away from Hamas. http://www.weeklystandard.com/blogs/israel-warns-journalists-stay-away-hamas_663755.html, November 2012. The Weekly Standard, retrieved 19 January 2013.

[21] 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.

[22] Aaron Hess. Resistance up in smoke: Analyzing the limitations of deliberation on YouTube. *Critical Studies in Media Communication*, 26(5):411–434, 2009.

[23] Noor Huijboom and Tijs Van den Broek. Open data: an international comparison of strategies. *European Journal of ePractice*, 12(1), 2011.

[24] M. Jacobson. Terrorist financing and the internet. *Studies in Conflict & Terrorism*, 33(4):353–363, 2010.

[25] G. Jinlan. Government websites optimization for rising in search engine ranking. *Journal of Modern Information*, 7:017, 2009.

[26] A.M. Kaplan and M. Haenlein. Users of the world, unite! The challenges and opportunities of Social Media. *Business horizons*, 53(1):59–68, 2010.

[27] Sanja Kelly and Sarah Cook (eds.). *Freedom on the net 2011: a global assessment of internet and digital media*. Freedom House, 2011.

[28] Isabel Kershner and Fares Akram. Ferocious Israeli Assault on Gaza Kills a Leader of Hamas. http://www.nytimes.com/2012/11/15/world/middleeast/israeli-strike-in-gaza-kills-the-military-leader-of-hamas.html?pagewanted=all, November 212. NY Times, retrieved 19 January 2013.

[29] J. Lagerkvist. Internet Ideotainment in the PRC: national responses to cultural globalization. *Journal of Contemporary China*, 17(54):121–140, 2008.

[30] Cong Li. E-government website optimization based on search engine. In *Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC), 2011 2nd International Conference on*, pages 6224 –6227, aug. 2011.

[31] Martin C Libicki. *Conquest in cyberspace: national security and information warfare*. Cambridge University Press, 2007.

[32] Jesse Lichtenstein. Digital Diplomacy. http://www.nytimes.com/2010/07/18/magazine/18web2-0-t.html?_r=3&, July 2010. NY Times, retrieved 18 January 2013.

[33] Maria Lipman and Nikolai Petrov. Obshchestvo i grazhdane v 2008–2010 gg. [Society and Citizens 2008–2010], 2010. Carnegie Moscow Center Working Papers, No. 3.

[34] Angela Maria Lungu. War. com: The internet and psychological operations. Technical report, Naval War College, 2001.

[35] E. Morozov. Technology’s role in revolution: Internet freedom and political oppression. *The Futurist*, 45(4):18–21, 2011.

[36] Evgeny Morozov. *The Net Delusion: How not to liberate the world*. Penguin, 2011.

[37] Asher Moses. PM’s staff sanitise Wikipedia. http://www.smh.com.au/news/technology/pms-staff-edited-wikipedia/2007/08/23/1187462441687.html?page=fullpage, August 2007. The Sydney Morning Herald, retrieved 19 January 2013.

[38] S. Nagaraja and R. Anderson. The snooping dragon: social-malware surveillance of the Tibetan movement, March 2009. Technical Report Number 746.

[39] *Allied Joint Doctrine for Information Operations, AJP-3.10*. NATO, 2009.

[40] Open Net Initiative. About filtering. http://opennet.net/about-filtering. Retrieved 14 November 2012.

[41] Ed Oswald. Researcher: US Gov't Editing Wikipedia Entries. http://betanews.com/2007/08/17/researcher-us-gov-t-editing-wikipedia-entries/, August 2007. Betanews, retrieved 19 January 2013.

[42] Nicole Perlroth. Google Warns of New State-Sponsored Cyberattack Targets. http://bits.blogs.nytimes.com/2012/10/02/google-warns-new-state-sponsored-cyberattack-targets/, October 2012. NY Times, retrieved 19 January 2013.

[43] Anas Qtiesh. Spam Bots Flooding Twitter to Drown Info About #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.

[44] J. Ratkiewicz, M. Conover, M. Meiss, B. Gonçalves, S. Patil, A. Flammini, and F. Menczer. Detecting and tracking the spread of astroturf memes in microblog streams. *arXiv preprint arXiv:1011.3768*, 2010.

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

[46] J. Rogoza. The Internet in Russia: The cradle of civil society, March 2012. OSW Commentary No 72.

[47] Random sample. *Science*, 339(6125):1258–1259, 2013.

[48] Noah Shachtman. Israel Kills Hamas Leader, Instantly Posts It to YouTube. http://www.wired.com/dangerroom/2012/11/idf-hamas-youtube/, November 2012. Wired, retrieved 20 January 2013.

[49] Thom Shanker and Eric Schmitt. Pentagon Weighs Use of Deception in a Broad Arena. http://www.nytimes.com/2004/12/13/politics/13info.html?_r=0, December 2004. NY Times, retrieved 19 January 2013.

[50] Ryan Singel. Juking Your Facebook 'Like' Stats Is as Easy as Sending a Message. http://www.wired.com/threatlevel/2012/10/facebook-likes-messages/, note=Wired, retrieved 18 January 2013, October 2012.

[51] Andrei Soldatov and Irina Borogan. The Kremlin’s New Internet Surveillance Plan Goes Live Today. http://www.wired.com/dangerroom/2012/11/russia-surveillance/, November 2012. Wired, retrieved 18 January 2013.

[52] Mark Sweney. Facebook quarterly report reveals 83m profiles are fake. http://www.guardian.co.uk/technology/2012/aug/02/facebook-83m-profiles-bogus-fake, August 2012. The Guardian, retrieved 18 January 2013.

[53] Daniel Terdiman. Report: Twitter hits half a billion tweets a day. http://news.cnet.com/8301-1023_3-57541566-93/report-twitter-hits-half-a-billion-tweets-a-day/, October 2012. CNET, retrieved 19 January 2013.

[54] T.L. Thomas. Countering internet extremism. *IO Sphere*, Winter 2009:16–21, 2009.

[55] Wikipedia, the free encyclopedia. http://en.wikipedia.org/wiki/Main_Page. Retrieved 19 January 2013.

[56] J. Zittrain and B. Edelman. Internet filtering in China. *Internet Computing, IEEE*, 7(2):70–77, 2003.

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