2014 6th International Conference on Cyber Conflict
P.Brangetto, M.Maybaum, J.Stinissen (Eds.)
2014 © NATO CCD COE Publications, Tallinn

Socio-Political Effects of Active Cyber Defence Measures

Keir Giles
Conflict Studies Research Centre
Oxford, UK
keir.giles@conflictstudies.org.uk

Kim Hartmann
Otto-von-Guericke-Universität
Magdeburg, Germany
kim.hartmann@ovgu.de

Abstract: This paper compares public and political attitudes across a range of countries to systems for monitoring and surveillance of internet usage. U.S. and Russian data collection and mining systems are taken as case studies. There are wide variations in societal acceptability of these systems based on the perceived acceptable balance between personal privacy and national security. Disclosures of covert internet monitoring by U.S. and other government agencies since mid-2013 have not led to a widespread public rejection of this capability in the U.S. or Europe, while in Russia, internet users show acceptance of limitations on privacy as normal and necessary. An incipient trend in EU states toward legitimisation of real-time internet monitoring is described.

Keywords: *active cyber defence, Russia, UK, monitoring, surveillance, US, PRISM, SORM*

1. INTRODUCTION

Like many other concepts relating to cyberspace, the term "Active Cyber Defence" at present lacks a universally accepted definition. But any such definition must encompass proactive measures in cyberspace for the purpose of incident prevention, and these measures must not necessarily be limited to technical means.[1] In this paper, we examine social and political, rather than technical, aspects of a national proactive cyber defence posture, by examining two sets of preventive measures related to monitoring and surveillance of an online population.

In China, as well as to some extent in Russia, misuse of social media is perceived as a significant national security issue. The perceived threat is from "the rapid growth of social networking and instant communication tools, like Weike and WeChat, which disseminate information rapidly,

1 According to one authoritative US official, cyber defence is the "ability to draw on the strengths of our partners and bring to bear the best technical skills against any existing or evolving threat. Effective cyber defenses ideally prevent an incident from taking place. Any other approach is simply reactive". See testimony to U.S. Committee on Homeland Security and Governmental Affairs by Sallie McDonald, Assistant Commissioner for the U.S. Office of Information Assurance and Critical Infrastructure Protection, published 31 July 2012, available at http://hsgac-amend.senate.gov/old_site/100401mcdonald.htm

have a large influence and broad coverage, and have a strong ability to mobilize society."[2] Close control of social media, and warning and punishing abusers in order to prevent uncontrolled distribution of information which is hostile to the ruling powers is a prime example of proactive online defence to protect national security.[3]

In this paper, one U.S. and one Russian online data collection and mining system intended to exploit the internet to defend against threats to national security will be reviewed. These two programmes, known to the public as PRISM and SORM respectively, are instructive not only because they demonstrate two different approaches to a similar problem set, but also because they were initiated and continue to be operated in two very different legal and social contexts. Thus conclusions can be drawn for the legal status, and social acceptability, of other possible active cyber defence measures relating to surveillance of online activity.

The paper will review considerations regarding the broad effects of PRISM and SORM on national and international security and privacy issues, as well as whether and where these programmes are operated entirely in accordance with national law. The range of public and official reaction to both these systems in various countries will also be considered, allowing conclusions to be drawn about the extent to which proactive measures would be palatable to public opinion in the future.

2. THE INTERNATIONAL DEBATE

Disclosures of alleged U.S. surveillance activities to the public by former National Security Agency (NSA) contractor Edward Snowden in June 2013 sparked heated international debate on telecommunications monitoring as an act of prevention (i.e. as a form of proactive defence). Public discussion in the U.S., Europe, Russia and beyond revealed widely varying societal attitudes to the issues involved.

Although during the early stages of disclosure public dismay and strident political disapproval was primarily directed at the NSA and its British counterpart, GCHQ, as the Snowden disclosures progressed it became increasingly evident that many other states had been engaging in their own analogous monitoring and surveillance programmes, constrained only by the limitations of geography, political ambition and budget.[4] In the words of one authoritative commentator, this reflected the "big difference between the public outrage of politicians and the day-to-day reality of intelligence co-operation between Americans and Europeans".[5]

According to Finnish Foreign Minister Erkki Tuomioja, "All states spy on each other… All states are also being spied upon."[6] And Russian Foreign Minister Sergey Lavrov is reported to have

2 Paul Mozur, "China Wants to Control Internet Even More", *Wall Street Journal*, November 15, 2013, http://blogs.wsj.com/chinarealtime/2013/11/15/china-wants-greater-internet-control-public-opinion-guidance/

3 Josh Chin And Paul Mozur, China Intensifies Social-Media Crackdown, *Wall Street Journal*, September 19, 2013, http://online.wsj.com/news/articles/SB10001424127887324807704579082940411106988

4 Nigel Inkster, "Snowden – myths and misapprehensions", IISS, 15 November 2013, http://www.iiss.org/en/politics%20and%20strategy/blogsections/2013-98d0/november-47b6/snowden-9dd1

5 Julian Lindley-French, "What U.S. Intelligence Really Says About Europe", Speaking Truth Unto Power, October 31, 2013, http://lindleyfrench.blogspot.co.uk/2013/10/what-us-intelligence-really-says-about.html

6 "Foreign Minister: All states involved in spying", Yle news, November 3, 2013, http://yle.fi/uutiset/foreign_minister_all_states_involved_in_spying/6914489

commented on the monitoring of world leaders' phones: "It's a little boring to even comment. I mean, really, everybody already knew."[7] But elsewhere, especially in Western Europe, calm and reasoned reaction from responsible politicians was strikingly rare. Well-informed British expert Nigel Inkster notes that "countries that considered themselves to have friendly relations with the United States but which [had] been the subject of U.S. covert intelligence collection... reacted with varying degrees of outrage – some of it real, but much of it manufactured either for domestic political reasons or in the hope of leveraging some policy advantage from U.S. discomfiture."[8]

Meanwhile, sections of the English-language media appointed themselves to the role of gatekeepers and arbiters, deciding for themselves what classified information they would release to the public, according to their own definitions of national security.[9] But this approach failed to reflect the overall attitudes of internet users in the Anglosphere, and even less so those of internet users overall.

The recent growth of non-Anglophone online populations has led to a rapid movement away from Euro-Atlantic views of the nature of the internet and how it and its freedoms should be regulated. In 1996, the U.S. made up over 66% of the world's online population, whereas in 2012, it accounted for only 12%.[10] According to one assessment, India saw an increase in numbers of internet users of 32% just in the year to March 2012.[11] One effect of this shift is an adjustment in median attitudes of internet users to the ideal balance of privacy against security on the internet. Russia provides a clear example of this different approach and set of assumptions by the broad mass of users,[12] and it is for this reason that this paper uses a Russian system to compare and contrast with U.S. surveillance programmes.

3. INTERNET SURVEILLANCE – TWO SYSTEMS COMPARED

In November 2013 a delegation of representatives of Russia's Federation Council (the parliament's upper house) and Foreign Ministry visited the U.S. with the intention of taking American service providers to task for not guaranteeing user privacy against government intrusion - a reversal of roles which six months earlier would have seemed laughable.[13] Yet the Snowden allegations conclusively dislodged the United States from the moral high ground of internet user freedom.

7 As reported by TIME's Moscow correspondent Simon Shuster on Twitter: https://twitter.com/shustry/status/395640131547189248

8 Nigel Inkster, "Snowden – myths and misapprehensions", IISS, 15 November 2013, http://www.iiss.org/en/politics%20and%20strategy/blogsections/2013-98d0/november-47b6/snowden-9dd1

9 "Guardian worldview at root of national security row", *The Commentator*, October 10, 2013, http://www.thecommentator.com/article/4250/guardian_worldview_at_root_of_national_security_row

10 "State of the Internet in Q3 2012", comScore, December 5, 2012, http://www.comscore.com/Insights/Presentations_and_Whitepapers/2012/State_of_the_Internet_in_Q3_2012

11 "State of the Internet in Q1 2012", comScore, available at http://www.slideshare.net/alcancemg/state-of-theinternetq12012webinar-copy

12 Keir Giles, "After Snowden, Russia Steps Up Internet Surveillance", Chatham House, October 29, 2013, http://www.chathamhouse.org/media/comment/view/195173

13 "U.S. ready to discuss cyber security with Russia - Ruslan Gattarov", Voice of Russia, November 15, 2013, http://voiceofrussia.com/2013_11_15/US-ready-to-discuss-cyber-security-with-Russia-Ruslan-Gattarov-6191/?print=1

A. PRISM

PRISM, an online mass electronic data collection tool operated by U.S. security agencies, was the first alleged classified monitoring and surveillance system to be made public by Snowden.[14] The word PRISM has since entered common usage as a shorthand for a whole range of different alleged U.S. surveillance and query mechanisms.[15] But for the purposes of this paper, reference will only be made to disclosures relating to this specific system. The description of this system below is drawn from media reporting, and it should be noted that no reported details have been confirmed, and furthermore much reporting on this topic substantially misunderstands and/or misrepresents the source documents. The details on PRISM repeated below are useful only to the extent that they reflect what has been presented to internet users worldwide, and they are the information on the basis of which public opinion has been formed.

It is important to note that according to the publicly available reports, PRISM is not an interception or intrusion but rather a data mining tool. This implies that PRISM is not used to break into personal computer systems, but analyses data. The data analysed is provided by companies providing internet or computing services. Hence, only data transferred to these companies is monitored by PRISM.

In June 2013, the Washington Post released a list of nine U.S. service providers known to have cooperated with the NSA. These companies were:

- **Microsoft.** In June 2013 Microsoft released a press statement claiming to have only forwarded data to the authorities if legitimised through a legally binding document.[16]

- **Google.** Google states that data is only being exchanged with the U.S. authorities when legally demanded.[17]

- **Facebook**, known originally as a social network only but expanding into other services and especially known for its massive data collection policies. Following Google, Facebook also stated that it only provides data to the U.S. authorities when legally obliged to do so.[18]

The remaining service providers were Apple, Youtube, Skype, AOL and Yahoo. Open source

14 Greenwald, Glenn and MacAskill, Ewen, "NSA Prism program taps in to user data of Apple, Google and others", *The Guardian*, June 6, 2013, http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

15 Gellman, Barton, "U.S. surveillance architecture includes collection of revealing Internet, phone metadata", *The Washington Post*, June 16, 2013, http://www.washingtonpost.com/investigations/us-surveillance-architecture-includes-collection-of-revealing-internet-phone-metadata/2013/06/15/e9bf004a-d511-11e2-b05f-3ea3f0e7bb5a_story.html

16 "Statement of Microsoft Corporation on Customer Privacy", Microsoft, June 6, 2013, http://www.microsoft.com/en-us/news/press/2013/jun13/06-06statement.aspx

17 Page, Larry and Drummond, David, "Official Google Blog", June 7, 2013, http://googleblog.blogspot.de/2013/06/what.html

18 Gellmann, Barton and Poitras, Laura, "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program", *The Washington Post*, June 6, 2013, http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?hpid=z1

reporting also suggested that Dropbox provided data for the PRISM programme, but Dropbox denies any knowledge of this.[19]

1) Technical Aspects

Being a data mining tool, PRISM relies heavily on multiple data sources. There are few technical details publicly available about the technical implementation of PRISM and its exact functions provided. However, as far as details are available, it seems that the collection process of PRISM is limited to providing an interface to request data from cooperating service providers. The requested data is then transferred from the service provider's database to local servers directly accessible by PRISM.

It is known that certain user actions (such as logging on or off) yield notifications in the system, initiating new data requests or suggesting the request to an operator. According to slides supposedly explaining PRISM published through the Washington Post, the data collection is initiated and operated through the FBI "Data Interception Technology Unit" (DITU). The DITU forwards the data to the NSA program "PRINTAURA" that seems to be used to control the traffic flow, passing it on to "SCISSORS" and "PROTOCOL EXPLOITATION S3132" used to distinguish between different data types (voice, video, call and internet records). The appropriate path (NUCLEON, PINWALE, MAINWAY or MARINA) is chosen accordingly for further processing/analysing of the obtained data. After having passed through these programs, the data is indexed according to a code containing information about the provider, type of data collected, source and date as well as a serial number.

The slides provided do not include information about when and how it is decided to add a user to the PRISM database, i.e. how it is decided to monitor a specific user continuously. However, this aspect is crucial to the public debate as it yields both privacy and ethical issues.

Once in the database, PRISM seems to automatically retrieve information about certain user actions, triggering a new data collection process. This implies that once a user is added to the database, legal actions such as logging in to the e-mail provider may trigger monitoring and data collection routines. The user is put under general suspicion. This practice is not uncommon in criminal investigations, but it seems that the legal barriers for the non-digital surveillance of individuals are higher than those for PRISM observations, yielding legal and ethical questions.[20]

2) Legal Aspects

PRISM was initiated by the Protect America Act under the administration of President George W. Bush. As PRISM collects data from companies under Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act 2008, PRISM is operated under the supervision of the U.S. Foreign Intelligence Surveillance Court (FISC).[21] FISA regulates procedures to physically and digitally monitor and collect foreign intelligence information. The monitoring may be extended to any individual being suspected of espionage or terrorism world-wide, although the law is not applicable outside the U.S.

19 Lardinois, Frederic, "Google, Facebook, Dropbox, Yahoo, Microsoft, Paltalk, AOL And Apple Deny Participation In NSA PRISM Surveillance Program", Tech Crunch, June 6, 2013, http://techcrunch.com/2013/06/06/google-facebook-apple-deny-participation-in-nsa-prism-program/

20 "NSA slides explain the PRISM data-collection program", *The Washington Post*, June 6, 2013. http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

21 "NSA slides explain the PRISM data-collection program", *The Washington Post*, June 6, 2013, http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

It should be noted that knowledge of this capability and its application was already in the public domain long before disclosures by Snowden. Reporting by the New York Times in December 2005 described how the Bush administration secretly authorized the NSA to eavesdrop on both Americans and other individuals within the U.S. in order to counteract terrorism without court-approved warrants. This amendment provided the NSA with the ability to decide on the monitoring of individuals without any further court-approval necessary. Although this report led to discussions within the U.S., including both official concerns over disclosure and public concerns over privacy which foreshadowed the much more substantial debates triggered by Snowden, there appears to have been little visible impact at that time outside the U.S.[22] Now, in 2013, the extent to which FISA has been used in order to monitor both foreigners and Americans has led to controversial discussion among lawmakers, lawyers and researchers both within the U.S. and abroad, with sharply divided opinions on both the legality and constitutionality of operations.[23]

B. SORM

In marked contrast to information on PRISM, which took many internet users by surprise, large parts of the Russian internet surveillance and monitoring system have been public knowledge since their inception.

While disclosure of the capabilities of U.S. monitoring systems including PRISM provoked widespread reactions of shock in Europe (whether genuine or otherwise), reactions in Russia were tempered by the knowledge that Russia has been operating the SORM system openly, and governed by laws and regulations which are publicly accessible, for over a decade. In short, in Russia, an online public that is entirely accustomed to being monitored by the state approached the problem with a different set of presumptions.

SORM, an abbreviation for *Sistema operativno-rozysknykh meropriyatiy*, or System for Operational Investigative Activities, is a well-documented and long-established system for monitoring use of the internet through Russian internet service providers (ISPs) and enabling access to this monitoring for a range of Russian law enforcement bodies. One important contrast with PRISM is that SORM is primarily directed at collection of communications data from all communications users within Russia, whereas PRISM is a global programme mining data from selected highly specific targets worldwide. In other words, while both PRISM and SORM are capable of monitoring foreign users' data, PRISM is part of an active collection programme which "goes outside" to collect data, while SORM is instead passive and waits for the data to get "inside" the Russian national network. It is still the case, however, that some international users may be just as unaware of their data being automatically monitored through SORM as they were unaware of the potential of being monitored through U.S. systems.

Thus the legality and public acceptability, or otherwise, of covert interception of foreign nations' telecommunications raises different considerations in the Russian case from that of the U.S. At present, SORM is the only Russian programme named in the public domain with which

22 Risen, James und Lichtblau, Eric, "Bush lets U.S. spy on callers without court", *The New York Times*, December 16, 2005, http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=print&_r=0

23 Donohue, Laura, "NSA surveillance may be legal - but it is unconstitutional", *The Washington Post*, http://www.washingtonpost.com/opinions/nsa-surveillance-may-be-legal--but-its-unconstitutional/2013/06/21/b9ddec20-d44d-11e2-a73e-826d299ff459_story.html

these comparisons can be drawn; the likelihood of a Russian Snowden emerging to disclose the extent of other Russian measures directed abroad seems remote.

Sampling of opinion among Russian internet users suggests an acceptance of SORM and similar programmes based on greater relative weight given to security concerns over personal privacy, and an implicit understanding that use of the internet means a renunciation of privacy.[24] It should be noted that a significant proportion of media coverage implying criticism of Russian monitoring arrangements derives from a single source, the husband-and-wife team of Andrei Soldatov and Irina Borogan, who write and are quoted extensively on SORM and its derivatives in both Russian and foreign media.[25] Without their contributions and opinions, the open source picture on Russian internet surveillance would look substantially different.

At the same time, when legitimate concerns over online privacy are raised in Russia, official responses to them can on occasion spectacularly miss the point. For example, since mid-2013, Russia has moved to strengthen the role of the Federal Security Service (FSB) in ensuring domestic cyber security, both institutionally and technically.[26] Under a draft order sponsored by the Russian Ministry of Communications, as of July 1st 2014, Russian ISPs may be obliged to store records of all data and activities of users processed for a period of 12 hours, with provision for direct and immediate access to this information by the FSB.[27] But, it was reported, this new level of intrusion would not compromise the right to privacy because "personal information would only be available to specific organisations" rather than being made public.[28]

One under-reported potential consequence of the new requirement for 12-hour storage of user activity is a compromise of the security of the stored data. The new regulations will place a substantial financial burden on ISPs,[29] who will be under pressure to store very large quantities of data as cheaply as possible, with consequences for its secure handling. This has the potential to make Russian ISPs tempting targets for espionage and criminal activity.

Further proposed national security measures include close surveillance of visitors to the Sochi Winter Olympics 2014. According to experienced observer Mark Galeotti, intensive monitoring of electronic communications at Sochi is likely to be used as a test case for rolling out more intrusive and extensive systems than SORM, to include deep packet inspection (DPI) capability.[30] Yet media reporting of the proposed measures within Russia, including by

24 "Вы теперь интернетом как будете пользоваться?", Kommersant, October 21, 2013, http://kommersant.ru/doc/2324794

25 For example, Shaun Walker, "Russia to monitor 'all communications' at Winter Olympics in Sochi", *The Guardian*, October 6, 2013, http://www.theguardian.com/world/2013/oct/06/russia-monitor-communications-sochi-winter-olympics?CMP=twt_gu, and Andrei Soldatov, "Russia's Spying Craze", *The Moscow Times*, October 31, 2013 http://www.themoscowtimes.com/opinion/article/russias-spying-craze/488773.html

26 ГД одобряет передачу ФСБ полномочий по интернет-безопасности RIA-Novosti, November 15, 2013, http://ria.ru/defense_safety/20131115/977204644.html

27 Владислав Ъ-Новый, Елена Ъ-Черненко, Роман Ъ-Рожков, "Федеральный сервер безопасности", *Kommersant*, 21 October 2013, http://kommersant.ru/doc/2324684

28 "Хинштейн: доступ ФСБ к интернет-трафику не нарушит тайну личной жизни", RIA-Novosti, October 21, 2013, http://ria.ru/defense_safety/20131021/971490496.html

29 Keir Giles, "After Snowden, Russia Steps Up Internet Surveillance", Chatham House, October 29, 2013, http://www.chathamhouse.org/media/comment/view/195173

30 Mark Galeotti, "On your marks, get set… intercept!", oDRussia, October 29, 2013, http://www.opendemocracy.net/od-russia/mark-galeotti/on-your-marks-get-set%E2%80%A6-intercept

independent media citing foreign sources, gave the impression of general indifference to plans for pervasive monitoring.

4. PERCEPTIONS OF INTERNET SURVEILLANCE

This section reviews and reflects on some of the remarkable international reactions to the debate on internet surveillance which was triggered within Europe by the Snowden defection. The selected examples demonstrate specific reactions by social groups and their leaders, which illustrate the implications of covert versus acknowledged internet monitoring and surveillance, depending on the socio-cultural background of the public. A clear distinction needs to be drawn between average societal attitudes overall, and the public reactions of leadership figures – with even sympathetic commentators noting "the EU's theatrical outraged reaction".[31]

A. Germany

Sudden and uncontrolled disclosure of monitoring and surveillance systems affecting Germany triggered interesting socio-political reactions, partly related to Germany's unique history in Europe as a nation previously divided into one state with a strong respect for individual rights, and another where state surveillance and control of the population were all-pervasive.

Although privacy and data protection are major concerns in modern Germany and treated as fundamental rights, the initial German reactions to disclosures of NSA internet monitoring activities were untroubled. In August 2013, Ronald Pofalla, Chief of Staff of the German Chancellery and Federal Minister for Special Affairs, stated that the NSA and GCHQ had acted in accordance with German law,[32] and that any scandal was now "over".[33]

Subsequently, however, it was reported in October 2013 that Chancellor Angela Merkel's personal mobile phone was under surveillance by U.S. agencies.[34] During investigation of what became known in Germany as the "Handygate affair", further monitoring of German citizens and leaders was revealed. Public disapprobation was fuelled by disconcerting allegations that the German Bundestag was being monitored from the nearby U.S. embassy. With the embassy under special protection by German police and military services, the suggestion that German taxes had been used to protect an installation spying on German leaders and citizens contributed to a strong public backlash against monitoring and surveillance activities.[35]

31 Bérénice Darnault, "Why the EU response to NSA leaks is contradictory", The World Outline, October 28, 2013, http://theworldoutline.com/2013/10/eus-response-nsa-leaks-spying-scandal-contradictory/

32 Carstens, Peter, "Pofalla: Amerikaner und Briten halten sich an deutsches Recht", Frankfurter Allgemeine Zeitung, August 1, 2013, http://www.faz.net/aktuell/politik/inland/spaehaffaere-pofalla-amerikaner-und-briten-halten-sich-an-deutsches-recht-12528037.html

33 "Pofalla erklärt NSA-Affäre für beendet", Die Zeit, August 12, 2013, http://www.zeit.de/politik/deutschland/2013-08/nsa-bnd-pofalla--bundestag-spaehaffaere-snowden-abkommen

34 "Zu Informationen, dass das Mobiltelefon der Bundeskanzlerin möglicherweise durch amerikanische Dienste überwacht wird", Bundesregierung Pressemitteilung, October 23, 2013, http://www.bundesregierung.de/Content/DE/Pressemitteilungen/BPA/2013/10/2013-10-23-merkel-handyueberwachung.html

35 Smale, Alison, "Anger Growing Among Allies on U.S. Spying", The New York Times. October 23, 2013, http://www.nytimes.com/2013/10/24/world/europe/united-states-disputes-reports-of-wiretapping-in-Europe.html?_r=0

Commentators compared early bland government assurances that all actions were legal, and a refusal to engage with public concerns, followed by sudden and shocking disclosures, to the erection of the Berlin Wall in 1961. With public concern directed primarily at the United States, and only occasional reminders that "the U.S. isn't the only country German intelligence believes may be spying on the country's leadership",[36], Germany was forced to remonstrate publicly with its U.S. allies, with further potential severe implications for future legitimate monitoring operations within Germany.[37]

B. Nordic States

Conversely, Nordic EU member states have challenged assumptions with their reactions in the aftermath of the Snowden defection. The debate in Nordic countries, which might ordinarily have been expected to be staunch advocates of privacy rights, has been tempered by a more specific threat perception and an acute awareness of the vulnerabilities of those states.[38] In Finland, news of a sophisticated attack and data breach at the Ministry for Foreign Affairs (MFA), which private sources blamed on Russia,[39] gave impetus to public discussion of possible new laws on legal intercept - with much of the debate focusing not on whether this should take place, but under which government agency it would best fit.[40] Swedish Foreign Minister Carl Bildt described cooperation with foreign intelligence services on communications intelligence gathering against Russia as "hardly sensational".[41] And authorities in Denmark felt sufficiently secure in the legitimacy of their work to pre-empt inaccurate reporting by journalists supplied with Snowden material by going on the record to describe previously classified collection programmes.[42]

C. United Kingdom

The British debate is coloured by the particular role of the UK in two key aspects of the 2013 disclosures on internet surveillance: the prominent role of GCHQ as a partner of the NSA in facilitating surveillance, and the prominent role of The Guardian newspaper in disseminating stolen classified information on alleged surveillance activities.

Public perception of internet surveillance by the authorities also differs in the UK. Polling suggests that "60% plus" say the intelligence services have the right amount of power to monitor activity on the internet or need more – even though there is a perceived need for more transparency and an "informed dialogue with the public".[43]

36 Anton Troianovski, "Germany to Boost Anti-Spy Efforts", *Wall Street Journal*, November 20, 2013, http://online.wsj.com/news/articles/SB10001424052702304791704579209740311164308

37 Troianovski, Anton, "Germany Warns of Repercussions from U.S. Spying", The Wall Street Journal, October 28, 2013, http://online.wsj.com/news/articles/SB10001424052702304200804579163760331107226

38 "Swedes 'not afraid' of internet surveillance", *The Local*, November 8, 2013, http://www.thelocal.se/20131108/swedes-not-worried-about-internet-surveillance-survey

39 Keir Giles, "Cyber Attack on Finland is a Warning for the EU", Chatham House, November 8, 2013, http://www.chathamhouse.org/media/comment/view/195392

40 "Verkkovalvonta keskittymässä yhdelle taholle", *Ilta-Sanomat*, 18 November 2013, http://m.iltasanomat.fi/kotimaa/art-1288622010437.html

41 "Bildt defends Sweden surveillance", *The Local*, November 3, 2013, http://www.thelocal.se/20131103/bildt-defends-sweden-surveillance

42 Claus Blok Thomsen, Jakob Sorgenfri Kjær, Jacob Svendsen, "Presset FE fortæller om dansk spionage", *Politiken*, November 20, 2013, http://politiken.dk/indland/ECE2138411/presset-fe-fortaeller-om-dansk-spionage/

43 UK Home Secretary Hazel Blears, speaking at Intelligence and Security Committee open evidence session, November 7, 2013, UK Parliament website, http://www.parliamentlive.tv/Main/Player.aspx?meetingId=14146

The appearance before Parliament's Intelligence and Security Committee of the chiefs of the three UK intelligence and security services[44] began a significant shift in public opinion.[45] Afterwards, there were indications that even the most liberal-minded of observers were beginning to realise the extent of the damage done by The Guardian's misguided crusade.[46] At the time of writing, unease at The Guardian's continued support for Snowden associate Glenn Greenwald was beginning to grow. This was aided by mistakes by both parties, including insistence on the palpably untrue assertion that limited damage had been done by releasing the files, since 850,000 individuals already had access to them,[47] and easily detected misinformation by Greenwald on the content of individual files, as in the case of allegations that millions of telephone calls in Norway had been intercepted by the NSA.[48] According to one expert assessment, Snowden "did not understand the significance of much of the material he did read and that the same was true for the newspapers that published it. The resulting confusion and misapprehensions that have taken hold within the media and shaped the public debate".[49]

Broadly, UK public opinion appears to be in line with the perception reflected in U.S. polls that releasing classified information on internet surveillance was harmful to national security[50] - to the palpable frustration of liberal journalists that the rest of the UK does not see it their way.[51] It has been argued that, in a curious parallel with Russia, this results from a higher British perception of the security interests that are at stake. As described in the Financial Times:

"The basic narrative of British history... is of a country that has had to ward off a succession of attempted foreign invasions. The role of the intelligence services in protecting the UK is both noted and celebrated… Most British citizens accept and, indeed, celebrate the role of the state in keeping the country free and independent – and the role of the intelligence services has historically been integral to that task. The threat from terrorism, as witnessed in the London bombings of 2005, has only increased the awareness of the need for good intelligence."[52]

44 Intelligence and Security Committee open evidence session, November 7, 2013, UK Parliament website, http://www.parliamentlive.tv/Main/Player.aspx?meetingId=14146

45 Catherine A. Traywick, "British Spies Aren't James Bonds, and 7 Other Things We Learned from Britain's Landmark Intelligence Hearing", Foreign Policy, November 7, 2013, http://blog.foreignpolicy.com/posts/2013/11/07/british_spies_arent_james_bonds_and_7_other_things_we_learned_from_the_uks_landmar

46 Andrew Sparrow, "Guardian faces fresh criticism over Edward Snowden revelations", *The Guardian*, November 10, 2013, http://www.theguardian.com/media/2013/nov/10/guardian-nsa-revelations-edward-snowden

47 Nicholas Watt, "Threat from NSA leaks may have been overstated by UK, says Lord Falconer", *The Guardian*, November 17, 2013, http://www.theguardian.com/world/2013/nov/17/threat-nsa-leaks-snowden-files

48 Kjetil Magne Sørenes, "Dette dokumentet viser ikke overvåking av Norge, ifølge E-tjenesten", *Dagbladet*, 19 November 2013, http://www.dagbladet.no/2013/11/19/nyheter/snowden_i_norge/edward_snowden/innenriks/samfunn/30395928/

49 Nigel Inkster, "Snowden – myths and misapprehensions", IISS, 15 November 2013, http://www.iiss.org/en/politics%20and%20strategy/blogsections/2013-98d0/november-47b6/snowden-9dd1

50 Scott Clement, "Poll: Most Americans say Snowden leaks harmed national security", *The Washington Post*, November 20, 2013, http://www.washingtonpost.com/politics/poll-most-americans-say-snowden-leaks-harmed-national-security/2013/11/20/13cc20b8-5229-11e3-9e2c-e1d01116fd98_story.html

51 John Naughton, "Edward Snowden: public indifference is the real enemy in the NSA affair", The Observer, October 20, 2013, http://www.theguardian.com/world/2013/oct/20/public-indifference-nsa-snowden-affair

52 Gideon Rachman, "Why the British like their spies", *Financial Times*, November 10, 2013.

5. CONSEQUENCES

The immediate consequence of Edward Snowden's distribution of classified information on alleged internet surveillance activities is a severe detriment to the national security of a number of states around the world. According to NSA Director General Keith Alexander the documents were "being put out in a way that does the maximum damage to NSA and our nation".[53] GCHQ Director Iain Lobban agrees, saying that the "cumulative effect of the global media coverage will make our job far, far harder for years to come".[54]

The defection of Snowden placed additional strain on an already challenging relationship between Russia and the U.S., with both sides expressing "disappointment" with each other, over Russia's acceptance of an application by Snowden for temporary asylum[55] and the subsequent decision by the U.S. to cancel a meeting between Presidents Obama and Putin scheduled for early September 2013.[56]

But the diplomatic effect extends beyond the U.S. and Europe. The Brazilian reaction to allegations of espionage by the USA and Canada was especially vehement.[57] Brazil will host a global conference on internet security in 2014 "to identify common objectives and ways of limiting espionage and monitoring operations".[58] Yet once again, there are indications that the outrage may be largely artificial. The suggestion that this came as a revelation to Brazil, giving rise to entirely new concerns, is belied by earlier plans for direct cable links with other countries "with the explicit aim of enhancing cyber security for the participating nations by bypassing the United States".[59]

In some cases, the diplomatic fallout has direct security consequences. For instance, diplomatic tensions between Australia and Indonesia peaked, reflected in an exchange of sexually lurid front-page cartoons in Australian and Indonesian newspapers, with the implication that surveillance of Indonesian targets "gave some kind of prurient pleasure to a brutish, hairy-legged Australia".[60] As a result, elements of intelligence cooperation between the two nations have been suspended, which is expected to result in an increased terrorism and criminal threat to Australia.[61]

53 Mark Hosenball, "NSA chief says Snowden leaked up to 200,000 secret documents", Reuters, November 14, 2013, http://www.reuters.com/article/2013/11/14/us-usa-security-nsa-idUSBRE9AD19B20131114

54 Sir Iain Lobban, Director, GCHQ, speaking at Intelligence and Security Committee open evidence session, November 7, 2013, UK Parliament website, http://www.parliamentlive.tv/Main/Player.aspx?meetingId=14146

55 Luhn, Alec, Harding, Luke and Lewis, Paul, "Edward Snowden asylum: U.S. 'disappointed' by Russian decision", *The Guardian*, August 2, 2013, http://www.theguardian.com/world/2013/aug/01/edward-snowden-asylum-us-disappointed

56 "Russia 'disappointed' bilateral talks with U.S. cancelled", BBC, August 7, 2013, http://www.bbc.co.uk/news/23608052

57 Tamara Santos, "Why is everyone spying on Brazil?", The World Outline, October 13, 2013, theworldoutline.com/2013/10/everyone-spying-brazil/

58 Tamara Santos, "Why is everyone spying on Brazil?", The World Outline, October 13, 2013, theworldoutline.com/2013/10/everyone-spying-brazil/

59 Keir Giles, "Russian Interests In Sub-Saharan Africa", U.S. Army War College Strategic Studies Institute, July 2013, p. 34.

60 Michael Bachelard, "Australia's reputation in Indonesia hits new low", *The Age*, November 23, 2013, http://m.theage.com.au/federal-politics/political-news/australias-reputation-in-indonesia-hits-new-low-20131123-2y2k2.html

61 John Schindler, "Snowden's Thunder Down Under", The XX Committee, November 21, 2013, http://20committee.com/2013/11/21/snowdens-thunder-down-under/

But in addition to the long-term national security implications, there have been direct and immediate consequences in both commercial and legal terms in a number of countries. "Fears about the NSA using American hardware to spy on the rest of the world"[62] have led to severe revenue implications for U.S. companies, with major players such as CISCO and IBM suffering badly.[63] As pointed out by Nigel Inkster, "the major U.S. technology companies and service providers which have to varying degrees collaborated with the NSA, either voluntarily or in response to judicial warrants, have experienced a decline in trust with uncertain but potentially significant implications for their future business prospects."[64] Businesses promoting cloud services in particular have reportedly experienced a significant drop in demand due to security fears, while firms in Switzerland are benefiting from that country's current perceived status as unaffected by surveillance concerns.[65]

Most significantly for the purposes of this paper, one trend that was beginning to be observed at the time of writing is the move towards public legitimisation of internet interception and surveillance activities.

A conference at London's Chatham House in late November 2013 heard how online activity worldwide was in effect being governed by U.S. law, while in the USA itself, the response to disclosures of NSA activities was calls across the political spectrum not for a reduction in the extent of surveillance, but for greater oversight of its implementation.[66] In its work with overseas intelligence-gathering organisations, the NSA had been restricted, or in some cases assisted, by very different legal environments in the partner country. An unattributed document released in December 2013 and purporting to review NSA cooperation agreements with a range of foreign partner organisations refers to "legal and policy impediments on the partner side".[67] In a possibly unrelated example, domestic legal considerations caused the Japanese government to decline NSA requests for cooperation in tapping cables carrying phone and Internet data across the Asia-Pacific region in 2011.[68] But after October 2013, a number of European countries have moved to establish or reinforce a firm legal framework for their own interception and surveillance activities.

There are numerous and varying assessments of the legality of interception of communications in Europe, even within the narrow focus of privacy as a human rights issue. According to a draft of the "EU Human Rights Guidelines on Freedom of Expression Online and Offline",

62 Christopher Mims, "Cisco's disastrous quarter shows how NSA spying could freeze U.S. companies out of a trillion-dollar opportunity", Quartz, November 14, 2013, http://qz.com/147313/ciscos-disastrous-quarter-shows-how-nsa-spying-could-freeze-us-companies-out-of-a-trillion-dollar-opportunity/

63 Cyrus Farivar, "Cisco attributes part of lowered earnings to China's anger toward NSA", Ars Technica, November 14, 2013, http://arstechnica.com/business/2013/11/cisco-attributes-part-of-lowered-earnings-to-chinas-anger-towards-nsa/

64 Nigel Inkster, "Snowden – myths and misapprehensions", IISS, 15 November 2013, http://www.iiss.org/en/politics%20and%20strategy/blogsections/2013-98d0/november-47b6/snowden-9dd1

65 Varying estimates given by multiple industry speakers at "e-Crime & Information Security Mid Year Meeting", London, October 24, 2013

66 "Power and Commerce in the Internet Age", Chatham House, London, November 25-26 2013, agenda available at http://www.chathamhouse.org/Internet2013/agenda

67 Unattributed document provided by Swedish SVT television's "Uppdrag Granskning" investigative programme, available at https://www.documentcloud.org/documents/894386-legal-issues-uk-regarding-sweden-and-quantum.html

68 "NSA asked Japan to tap regionwide fiber-optic cables in 2011", *The Japan Times*, October 27, 2013, http://www.japantimes.co.jp/news/2013/10/27/world/nsa-asked-japan-to-tap-regionwide-fiber-optic-cables-in-2011/#.UnqQx3B7KsY

"lack of respect for the right of privacy and data protection constitutes a restriction of freedom of expression. Illegal surveillance of communications, their interception, as well as the illegal collection of personal data violates the right to privacy and freedom of expression."[69]

Yet in 2007, the European Court of Human Rights ruled as inadmissible (manifestly ill-founded) a complaint by an Italian internet user under Article 8 (right to respect for private and family life) of the European Convention on Human Rights. Although the complaint related to spam rather than surveillance, the Court declared that "once connected to the Internet, e-mail users no longer enjoyed effective protection of their privacy".[70]

As noted above, a cyber attack on the Finnish Ministry for Foreign Affairs (MFA) spurred attempts there to legitimise active defence, in the form of pre-emptively screening both data traffic within Finland and that which passes through Finnish cables, as opposed to the current state of legislation where data can only be intercepted once a crime is suspected and an investigation in progress. The aim, according to the Finnish Minister of Defence, would be to enable Finland "to prevent and intervene if another country's intelligence operations focus on Finland and Finnish officials."[71]

In an apparent direct reference to the MFA attack, which Finland learned of through a tipoff from Sweden's FRA signals intelligence agency, National Police Commissioner Mikko Paatero noted that "we cannot follow signals in Finland or travelling through Finnish cables... but others can do it for Finland. In my opinion it's a little bit embarrassing that we can hear from somewhere else about what is happening here."[72] Meanwhile in Sweden, although interception is already legal under the "FRA Law", the authorities are now seeking to enhance their powers in a similar manner to Russia.[73]

Most recently at the time of writing, a law was passed in France in December 2013 allowing surveillance of internet users in real time and without prior legal authorisation, by a much increased range of public officials including police, gendarmes, intelligence and anti-terrorist agencies as well as several government ministries.[74] The law gave rise to accusations of cynicism, being passed just weeks after France expressed outrage that the NSA had allegedly been engaged in similar activities, at which President François Hollande expressed his "extreme reprobation".[75]

69 Draft "EU Human Rights Guidelines on Freedom of Expression Online and Offline", unpublished, version as at November 20, 2013.

70 Muscio v. Italy, European Court of Human Rights, "Information Note on the Court's case-law No. 102", November 2007, http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=002-2419

71 "Defence Minister: Police and defence forces to get wider web powers", Yle News, November 2, 2013, http://yle.fi/uutiset/defence_minister_police_and_defence_forces_to_get_wider_web_powers/6914546?origin=rss

72 "Finnish Police want web snooping powers", Yle news, November 7, 2013, http://yle.fi/uutiset/finnish_police_want_web_snooping_powers/6923309

73 "Intel agency seeks direct access to Swedes' data", *The Local*, November 19, 2013, http://www.thelocal.se/20131119/swedens-security-service-seeks-direct-data-access

74 "Adoption de la loi controversée de programmation militaire", *Le Monde*, December 10, 2013, http://www.lemonde.fr/international/article/2013/12/10/adoption-definitive-de-la-controverse-loi-de-programmation-militaire_3528927_3210.html

75 Kim Willsher, "French officials can monitor internet users in real time under new law", *The Guardian*, December 11, 2013, http://www.theguardian.com/world/2013/dec/11/french-officials-internet-users-real-time-law

In this way, disclosure of alleged surveillance activities by the NSA and GCHQ is having the effect, probably unanticipated by the disclosers, of ensuring that more of the U.S. and UK's partner nations are ensuring they have the legal framework in place to be able to participate in this activity on an unarguably legitimate basis.

6. CONCLUSION

Comparison of Russian, U.S. and British attitudes to internet monitoring demonstrates clearly that the common perception of legitimacy of that monitoring varies widely between nations.

Varying reactions to prior knowledge of Russian, and sudden disclosure of U.S. monitoring systems demonstrate that public responses are heavily influenced not only by national attitudes towards public security, but also by the extent of awareness of monitoring. A balance needs to be sought between the positive benefits of public knowledge of the precise limitations of privacy online, and the negative national and international security implications of widespread awareness of monitoring capabilities.

Direct comparison of the public reactions to PRISM and SORM supports this conclusion. Criticism of the aims and methods of PRISM and related systems was fuelled by their necessary lack of transparency. Failure to initiate public discussion about the nature of the threats which PRISM is intended to counter, and the nature of the counter-measures required, left the field open for wide-ranging and misinformed speculation. In particular, media coverage downplayed the legal controls and safeguards in place to protect the domestic US population from abuses of these capabilities. This situation was exacerbated by restraints on the U.S. intelligence community, which has been prevented from joining or contributing to the public narrative to correct speculation by the need to preserve what secrecy remains by not confirming or denying the accuracy of media allegations. By contrast, SORM is a system publicly avowed in the context of a well-developed threat narrative, and consequently does not excite similar reactions or wildly misinformed reporting.

Although disclosure of the alleged capability and reach of U.S. and allied surveillance mechanisms prompted strident and outraged reportage in some sections of the English-language media, public opinion has not followed suit. Instead, a more balanced and sober assessment of national security needs is leading European states to pass legislation through due democratic process to ensure that internet monitoring of specific threats to security continues unhindered. It follows that active cyber defence in the sense of active measures online in order to prevent and pre-empt threats to national security will continue to be perceived as legitimate, and these measures should be expected to continue unrestrained by the new environment of enhanced public awareness.