The Dogmata of Secrecy: Are we Realistic about the Facts and Impact of Massive Leaks of Classified Information?

C.N.J. de Vey Mestdagh[1],* et al[2]

1 Centre for Law&ICT, University of Groningen, the Netherlands; E-mail: c.n.j.de.vey.mestdagh@law-and-ict.org;

2 A. Kamphorst, J.H. Noordhoek, T. Mulder, H.T. van der Waaij; (Research) master and bachelor students Law&ICT and European and International Law at the University of Groningen, the Netherlands

* Invited and corresponding author

Abstract* – *In recent years, massive leaks of classified information enabled by the Internet have been at the core of political and media attention. Wikileaks and the Snowden files are well known examples. Public and political opinions show a particular black-and-white division. On the one hand there is alarm about the abuse of powers by intelligence services and on the other hand about the possible risks to national security. If we look at the fact finding side of the latter position there appears to be a vacuum. Opinion and not factual or logical proof is dominating the debate at this side. The dogmata of secrecy seem to prohibit such proofs. How can we elevate this debate by obtaining some facts and dependable conclusions in spite of their formal secrecy? In this paper we describe some methods available to perform the research necessary to answer this question and we will start making an inventory of press, political and scientific sources about the Snowden files to be able to estimate the actual as opposed to the alleged security impact of this case of massive leaking of classified information.

Keywords – Snowden; NSA; Leaks; Intelligence; Classified; Secrecy; Security; Transparency; Methodology;

1. The Dogmata of Secrecy

In all worlds in which propositions p and q are true the proposition p strictly implies q is contingent. So in our world where nuclear arms are evidently present since August 6, 1945 and a world war is absent since August 15, 1945 the proposition that nuclear arms strictly imply the absence of a world war is just contingent. To resolve the contingency in this case the hypothesis of deterrence should be falsified or its strength statistically tested. This hypothesis has fortunately neither been falsified nor has its strength ever been tested statistically. In the case of the alleged implication of certain consequences of massive leaks of classified information the position of its proposers is even worse. In the case of nuclear arms there is no doubt about their existence and - if used - their technical consequences nor about the absence of a world war. In the case of massive leaks of classified information there appears to be no oversight of the leaked information and there are no dependable sources for the alleged security consequences. Therefore, the many political and journalistic hypotheses about the alleged security consequences of these leaks are not only not falsified and not tested but at this moment - by lack of data - unfalsifiable and untestable.

This can legally and psychologically be explained by what we identified as the 'five dogmata of secrecy'[1]:

Dogma 1: It is self-evident that we need a secret service;
Dogma 2: It is also self-evident that the secret service is effective;
Dogma 3: We do not need independent research nor data or statistics to support dogma 2 (threats to (national) security suffice);
Dogma 4: The supervision of the secret services can be based on trust;
Dogma 5: We can proceed in the traditional way regardless of technical developments. Secret services (co)operate in a globalized information society but it is sufficient that they are only locally accountable.

The research described in this paper is inspired by the initial observation that there is a strong unbalance between the different public positions taken in the discussion about the implications of the Snowden files. On the one hand the position that intelligence services stretch their powers within and even beyond legal limits is well documented. On the other hand, the position that national security is threatened appears to be undocumented.[2] Since these positions require opposite political and legal arrangements - more oversight of secret services vs more powers for secret services - the answer to the following research questions is important. What methods could be used to document the confirmation or the negation of the latter position? What are the results of their application? What are the requirements for effective further research and what further research is necessary?

2. Methodology

What method can be used to circumvent the problems the dogmata of secrecy pose for research into the security consequences of the leaking of classified information?

To corroborate claims that the disclosure of classified information has certain consequences some conditions have to be met:

(1) The classified information must be available;
(2) The alleged consequences must have actually occurred;
(3) The relation between information and consequences must be theoretically possible, i.e. a coherent explanation has to be present or presented;
(4) To be convincing, this relation must be logically necessary, theoretically necessary – have no (serious) competition of theoretically possible alternatives) – or, if enough data are available, the relation must be probable or at least conventionally plausible, i.e. uncontested.

[1] cf. de Vey Mestdagh, 2015 [30].
[2] Fenster (2012) reaches a similar conclusion in the Wikileaks case [21].

Interestingly enough the research described in §3. of this paper strongly suggests that just one of these conditions has been met in the case of the alleged security consequences of the Snowden files.[3] The classified information appears to be only partially and selectively available. Many of the claims are based on information that is not available or not explicitly extracted from the available sources. Most of the consequences for security are still in the phase of allegation and not of proven occurrence. The claimed relations are not logically or theoretically necessary. In the absence of data, the probability of the relations cannot be estimated and even the supposed relations are highly contested.

The current debate about the security implications of the Snowden files is therefore based on the theoretical possibility of a relation between partially unknown or undisclosed information and unproven consequences.

This research has been set up to try to change this inexpedient situation. The first step was to make an inventory of possible sources of data. The second step was to define ways of exploring these data. And the final step was – if accessible – to actually search them.

Possible sources of data:

(1) The Snowden files;
(2) Public media (political and journalistic publications);
(3) Publicly available documents of governments and specifically secret services;
(4) Scientific publications;
(5) Technological information.

Ways of exploring these data:

(1) Find data in the Snowden files that inevitably (by logic or by lack of competition) lead to certain consequences;
(2) Make an overview of political and journalistic statements (pro and con);
(3) Find evidence in the publicly available accounts of governments and specifically secret services that harm has been done;
(4) Make documents of governments available, if necessary by exerting rights based on administrative transparency acts;
(5) Use the scientific work of others to reach conclusions;
(6) Infer that certain facts are technically impossible, e.g. by timeline, or implausible by competition.[4]

We will find out if this methodology can help us to circumvent the problem the dogmata of secrecy pose, by applying it. The aims of this research are ambitious and can only be attained over a longer period of time and through cooperation with journalists and other research groups. We made a start with a thorough inventory of the available Snowden files (§3.1.), the public media (§3.2.), literature (§3.3.) and public accounts of secret services in the Unites States of America (USA), the United Kingdom (UK) and the Netherlands (§3.4.).

3. Sources

First we did a search of the Snowden files to find facts that could entail security consequences ([1]..[7]). Next, we searched the public media to define the dominant opinions and to find analyses of facts and actual consequences and proposals for the reliable assessment of their interrelationship ([8]..[14]). Opinions are abundant, but analyses are missing. Therefore, the next step was searching for these missing analyses and proposals in literature ([15]..[29]). We found many historical descriptions and some theoretical analyses of the developments in the Snowden case but no factual substantiation of opinions or proposals for reliable research. We therefore conducted a systematic search for facts in the intelligence and security archives of the USA ([31]..[38]), the UK ([39]..[45]) and the Netherlands ([46]..[54]) over the period of the first publication of the Snowden files to August 2016. Our research in the archives of the services and the supervisory commissions did not produce facts, not even 'concrete' abstractions of facts. Finally, we did an incidental preliminary research to establish the viability of logical and technical methods to enhance the quality of the debate. We did a technology check on the position that the Snowden files were a condition sine qua non for the Paris terrorist attacks. Our conclusion is that the argument fails on the basis of the ample availability of the technology used before the publication of these files. This therefore seems a viable method for systematic further research.

3.1. The Snowden Files

A fundamental problem for our research is the incomplete and inadequate, often indirect, access to the fundamental facts.

Incomplete simply means that according to the available sources Snowden took between 58.000 and more than 1.5 million files.[5] According to Cryptome (2013, [4]) only 7,302 pages of the Guardian's first reported 58,000 files have been published, while according to the Canadian Journalists for Free Expression (2016, [2]) no more than 1182 documents have been made available.

[3] Of course in other cases the facts and consequences are proven, i.e. the facts that hurt the reputation of the NSA and other secret services, the effects this had on the attitudes of oversight organizations and public opinion and some political (cf. European Parliament, 2013 [20]), legal (cf. CJEU 2015, October 6, C-362/14) and economic (cf. Clark et al, 2013 [19]; Castro & McQuinn, 2015 [18]) effects.

[4] An example of a technical impossibility is that something happened before it occurred (the terrorists used a technique before 2013 that was only revealed by the Snowden files in 2013). An example of an implausibility is the assertion that a phenomenon has an exceptional cause instead of a commonly acknowledged cause (the terrorists used a technique that was widely known and very common before 2013 only because of the publication of the Snowden files in 2013). See §3.2.

[5] House of Representatives, USA. *Executive Summary of Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden* (2016, September 15), [32].

Inadequate, because journalists with access to the Snowden files have made a small opiniated selection of the files concerned with. For example, the cooperation of Verizon and other American telephone and IT companies with the NSA, the Prism programme, the NSA spying on foreign countries and world leaders and the interception by the NSA of text messages and phone calls, have been selected. However, we are not interested in the deduction of behaviours of our secret services, but in the corroboration of their propositions about the security consequences of these revelations. The Snowden files cannot provide that, being the alleged cause of these consequences. What they could provide is proof of the existence of the alleged causing facts.

What do we know? We know that the Snowden files are mainly NSA documents. We hardly have access to the original files. We do not even have a systematic inventory of their contents. Estimates of their number range from tens of thousands to more than a million. Actual access is limited to a small number of these documents and in most cases not the most revealing ones. For example, SIDtoday, the internal newsletter for the NSA's Signals Intelligence Directorate, which is partly published by Intercept (2016, [7]). The exception to this could be the revelation of the actual unknown trade of the secret services. However, the fact that secret services are tapping communications is not a revelation, but a confirmation of what secret services lawfully or unlawfully do. The former deputy head of MI6, Nigel Inkster, stated for example: '*I sense that those most interested in the activities of the NSA and GCHQ have not been told much they didn't already know or could have inferred*'.[6] In the case of cryptography there are even arguments to dismiss the relation between publication of the Snowden files and security consequences (see §3.2. below).

The reason for the scarcity of available Snowden files is not the unavailability of the files themselves but the selection which is made by the journalists involved. Glenn Greenwald writes: '*From the time we began reporting* […] *we sought to fulfill his* [Snowden's] *two principal requests* […]*: that they* [the files] *be released in conjunction with careful reporting that puts the documents in context and makes them digestible to the public*,[…] *and that the welfare and reputations of innocent people be safeguarded*.'[7] If it is true that certain individuals are more able to fulfil these requests than others, one should expect that these individuals share this burden with more of these able others in order to speed up the process of responsible publication.

3.2. Public Media

Our fact finding mission continued with a search through public media to be able to make an inventory of the dominant opinions about the consequences of the publication of the Snowden files and to analyse their foundations. We decided to include the Guardian [10], the Washington Post [13] and Der Spiegel [9] because of their involvement in the original publication of stories based on the Snowden files and to get international spread. We added the Intercept [11] because of their role as a platform for further publications about the Snowden files and for opening up an archive containing a small selection of the Snowden files. To extend our spread we added two large middle market newspapers USA Today [14], one of the widest circulated newspapers in the USA and the Telegraaf [8], the largest Dutch daily morning newspaper. We did a search in the archives of all of these media from the time of the first publications until August 2016. To complete this part of our research we scanned the available publications in one large down-market British newspaper, the Sun [12]. The conclusion of this search is that two political opinions are very dominant: amongst - former - government officials (1) *the massive information leaks are a serious threat to intelligence and security*; and amongst journalists (2) *governments massively abuse their powers through their Intelligence and Security Services*. Most of the journalistic comments follow this simple black and white scheme. Criticism is mainly directed at the lack of factual and theoretical underpinning of the opposite political opinions. Systematic analyses of data sources and criticism on - the lack of - methodology used or proposals for a reliable methodology are hard to find.

We shortly followed an interesting side track, because of its importance for further research. In a CNN interview about the Paris attacks with the former head of the CIA James Woolsey, the interviewer stated: '[…] *and they believe they knew to use encrypted communications because of the Edward Snowden revelations.*' Woolsey reacted: '[…] *I think the blood of a lot of these French young people is on his* hands [interviewer: '*because of what he revealed'*] *because of what he turned loose.*'[8] It can easily be shown from public sources that cryptography was available years before the Paris attacks and also propagated and used by terrorist networks.[9] Arguments that try to substantiate the relation between the Snowden files and the use of cryptography by terrorists all suffer from the Post hoc ergo propter hoc fallacy (cf. Shafer, 2014 [27], Adrian Cully in Verkaik, 2015 [29] and Recorded Future, 2014 [25]). This is an example of the kind of further research into technological facts and the methodical use of inferred impossibilities and implausibilities which can help to circumvent the effects of the dogmata of secrecy.

[6] Harding, 2014 [24]. See also Berghel, 2014 [16].

[7] Greenwald, G. (2016, May 16). The Intercept is Broadening Access to the Snowden Archive. Here's why. *The Intercept*. Retrieved from https://theintercept.com/2016/05/16/the-intercept-is-broadening-access-to-the-snowden-archive-heres-why/, [11].

[8] http://www.cnn.com/videos/us/2015/11/19/ex-cia-director-james-woolsey-edward-snowden-intvw-nr.cnn.

[9] Cf. United Nations Office on Drugs and Crime, 2012 [28]; Al-Qaeda in the Arabian Peninsula. *Inspire Magazine*. Summer 2010 and Fall 2010 issues [15]; Flashpoint Global partners, 2014 [22]; Hussain, M. (2014, September 16). No, Snowden's Leaks Didn't Help The Terrorists. *The Intercept*. Retrieved from https://theintercept.com/2014/09/16/snowdens-leaks-didnt-help-terrorists/, [11].

3.3. Literature

We searched SmartCat, Google Scholar and PiCarta to make an inventory of literature about the Snowden files. We also searched the internet libraries of the oversight organizations mentioned in the next paragraph for literature references. We were not able to access the National Security Archive because our institution has not signed up yet. We did however use the links in the article of Richelson (2013, [26]) to get access to a number of relevant files in this archive. This search has mainly been limited to the post Snowden years 2013- 2016. We read more than two hundred possibly relevant publications, including a few additional media publications and documents from the parliamentary archives of the USA, the UK and the Netherlands. We skipped all publications that were irrelevant to our research, for example publications about the behaviours of the NSA and other security services, the wilful cooperation of ICT companies, the events surrounding the leaking of the Snowden files, Edward Snowden as a person and the legal accountability of Edward Snowden. Finally, we concentrated on the thus selected publications about the contents of the Snowden files and its alleged consequences for national security. Apart from some of the sources referred to in §3.2., we did not find any serious, let alone scientific, research into actual or potential facts underpinning the alleged security risks. In most of the publications, the maximum of relevance can be summarized as follows: there is an alleged security risk and I know for a fact, or I think, or it is theoretically possible, or I believe that there is/there is no security risk without being specific about the antecedents or with nonfactual antecedents (see amongst others documents 65,[10] 71, 88, 92 and 112 included in Richelson, 2013 [26]). Facts - the content of specific Snowden documents hypothetically related to documented implications for security - are absent. We included a selection of the literature searched in our list of references ([15]..[29]) to give the reader an impression of common sources and we invite everyone to try to find the facts we are missing.

3.4. Intelligence Archives

The main focus of our current research has been a systematic and full search of the public archives of the oversight organizations concerned with intelligence activities in the USA, the UK and the Netherlands. We searched for factual evidence for the statements made about the consequences of Snowden's revelations. The position that these facts are classified and therefore probably cannot be found is justified, but does not generalize to the position that an abstraction of facts to a certain level, such as a class of facts, is also classified. It suffices to report that there are hard facts about a class of the alleged damages done to security and that the relation between these facts and the actual contents of certain published Snowden files can be established by following a particular explicit line of theoretical argument which has no serious competition. The actual classified facts can even confidentially be reported by the intelligence services to the assigned national supervisory commissions, who can translate them to the aforementioned level of abstraction in their reports to national parliaments. This would for example justify the demands for an increase of funding of intelligence agencies and of their investigative powers. Therefore, abstract statements that explicitly refer to undisclosed facts were included in the search. We did research in the archives from the time of the first publications of the Snowden files until August 2016. In none of the selected countries one can get direct access to documents of the secret services, with the exception of some noncommittal annual reports. So what we call intelligence archives are the publicly available proceedings of the supervisory national organizations to which the national secret services give account.

3.4.1. United States of America

The actual number of government organizations involved in intelligence activities in the USA is unknown.[11] The United States Intelligence Community (IC) is a federation of sixteen or seventeen - including the Office of the Director of National Intelligence - separate United States government agencies that work separately and together to conduct intelligence activities.[12] Executive oversight of these organizations is given to the President's Foreign Intelligence Advisory Board (PFIAB), the Joint Intelligence Community Council, the Office of the Inspector General (OIG; https://www.oig.doc.gov), and the Office of Management and Budget (https://www.whitehouse.gov/omb). Congressional oversight of the IC is assigned to the United States House Permanent Select Committee on Intelligence (HPSCI; http://intelligence.house.gov) and the United States Senate Select Committee on Intelligence (SSCI; https://www.intelligence.senate.gov/). There are no public archives of the executive oversight available. We searched the archives of the Congressional Select Committees on Intelligence, the House Committee on Armed Services, the House Committee on Homeland Security, the House Committee on the Judiciary, the Senate Committee on Homeland Security and Governmental Affairs and the Senate Committee on Foreign Relations ([31]..[38]). The pattern that emerges is that these committees are very concerned about the security consequences. This concern appears to be fully based on the opinions of IC officials and not on explicit or abstracted facts. We illustrate this pattern below by a selection of representative quotes from the committee's archives.

[10] In this document, by exception, there is a reference to a specific Snowden file. J.R. Clapper: '*The unauthorized disclosure of a top secret U.S. court document threatens potentially long-lasting and irreversible harm to our ability to identify and respond to the many threats facing our nation*'.

[11] 1,271 US government organizations are involved in intelligence activities, according to Priest, D., & Arkin, W. M. (2010, July 19). A hidden world, growing beyond control. *The Washington Post*, [13].

[12] See https://www.dni.gov/index.php/intelligence-community/members-of-the-ic and http://intelligence.house.gov/about/history-and-jurisdiction.htm.

House Permanent Select Committee on Intelligence

The position of the HPSCI becomes clear in their Annual Report of 29 December 2014 (H.Rep. 113-717, p.3, [31]). The bulk metadata program that was revealed by the Snowden files was *highly classified*, is *legal* and the NSA protected the constitutional rights of *U.S. persons*. The disclosure has caused damage to national security *that cannot be calculated and which may not become apparent for years.* Although perfectly *effective and legal*, public concern suffices to *end the bulk collection of telephone metadata, while preserving as much of the operational effectiveness and flexibility of the* [bulk metadata] *program.*

The HPSCI suggests that facts and consequences are known. '*This year, massive unauthorized disclosures of classified information caused immense damage to our national security*' (H.Rep. 113-277, p.9, [32]). However, this statement is not accompanied by even abstract classifications of the information and the damage or by any theoretical argument for a relation between these undisclosed information and damages.

On 15 September 2016, the House of Representatives published the HPSCI Executive Summary of Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden [32]. According to this report, '*Snowden caused tremendous damage to national security*'. '*Some of Snowden's disclosures exacerbated and accelerated existing trends that diminished the IC's capabilities to collect against legitimate foreign intelligence targets, while others resulted in the loss of intelligence streams that had saved American lives*.' We thought to get some concrete abstractions at last but then the argument deteriorates: '*The full scope of the damage inflicted by Snowden remains unknown.* […] *The Committee is concerned that the IC does not plan to assess the damage of the vast majority of documents Snowden removed.*' Our question is: If all of the reviewed operations have been compromised and its details are handed over to terrorists and nation states why should the oversight organizations be kept uninformed and ultimately the people be kept ignorant? One of the principal sources of the Review is the IC. The IC should not advise the House of Representatives or the HPSCI but be supervised by it. The IC is marking its own paper. Quis custodiet ipsos custodes?[13]

United States Senate Select Committee

Saxby Chambliss of the SSCI is well aware of at least a part of the limitations of the oversight method applied: '*We cannot do the oversight the American people expect of us if every request for information becomes a protracted battle.*' (S.Hrg. 113-89, 2013, March 12, p.4, [35]).

A different tone is chosen after the first leaks of the Snowden files: '*The Committee is dismayed by leaks that have appeared in the media* […] *The public disclosure of these programs* […] *has done grievous harm to the effectiveness of the programs involved and, hence, the nation's security.* […] *Up until these programs were leaked, their implementation by NSA was an example of how our democratic system of checks and balances is intended to, and does, work*' (S.Rep. 113-119,2013, November 12, p.3, [37]). So the system works fine. This change of tone would be understandable if the IC changed its ways and was providing adequate information.

The following quote suggests that adequate information is provided by the IC: '*The unauthorized disclosures concerning these lawful programs have provided al Qa'ida and others with a roadmap of how to better evade U.S. intelligence collection.* […], *the programs at issue become substantially less effective.*' (S.Rep. 113-119, 2013, November 12, p.4, [37]).

However, the SSCI applies the same method as the HPSCI. The IC is marking its own paper without providing any facts. '*As Director Olsen recently acknowledged, these disclosures have caused terrorist groups to change their communication methods and in other cases drop out of our collection altogether.*' (S.Hrg. 113-600, 2014, January 29, p.3, [35]). The source of this conviction is Director Olsen of the National Counterterrorism Center (NCTC; https://www.nctc.gov). James R. Clapper, Director of National Intelligence (DNI, https://www.dni.gov): '*But what I do want to speak to* […] *is the profound damage that his disclosures have caused and continue to cause. As a consequence, the nation is less safe and its people less secure.* […] *As a result, we've lost critical foreign intelligence collection sources, including some shared with us by valued partners.*[14] *Terrorists and other adversaries of this country are going to school on U.S. intelligence sources' methods and trade craft and the insights that they are gaining are making our job much, much harder. And this includes putting the lives of members or assets of the Intelligence Community at risk, as well as our armed forces, diplomats, and our citizens. We're beginning to see changes in the communications behavior of adversaries,*[15]' (S.Hrg. 113-600, 2014, January 29, p.5. [35]).

Next, the cogency of the convictions of the members of the IC is undermined further:
Director Clapper, DNI: '*It's clear as well that our collection capabilities are not as robust, perhaps, as they were because the terrorists—and* ***this is not specifically because of the Snowden revelations****—but generally have gotten smarter about how we go about our business and how we use trade-craft to detect them and to thwart them.*' (S.Hrg. 113-600, 2014, January 29, p41. [35]).

Director Olsen, NCTC: '*It certainly puts us at* ***risk of missing something*** *that* ***we are trying to see****, which could lead to putting us at* ***risk of an attack****, yes.*' Senator Collins: '*And just to quote you back to yourself, you said, 'This is not an exaggeration;* ***this is a fact.***' *And you*

[13] Juvenal, Satires (6, 347), Bochel, H., Defty, A., & Kirkpatrick, J. (2014) [17].

[14] One of these foreign intelligence collection sources is probably the Dutch GISS who unlawfully exchanged telephone metadata with the NSA. See §3.4.3. below.

[15] See §3.2. for an example of the fallacies that come with this kind of argument.

stand by that.' Director Olsen: *'I absolutely do, **yes**.'* (S.Hrg. 113-600, 2014, January 29, p. 50, [35]). In this quote it becomes obvious that the distinction between hypothetical and fact is not clear. The *risk* of missing *something* we are *trying* to see, which *could* lead to putting us at risk … is a hypothetical and not a fact.

Senator Rubio: *'Are there men and women in uniform who are potentially in harm's way because of what this individual has done?'* Lt. General Flynn, director Defense Intelligence Agency (DIA): *'Senator, I **believe** there are.'* (S.Hrg. 113-600, 2014, January 29, p.61, [35]). So facts become hypotheticals and hypotheticals become beliefs.[16]

3.4.2. United Kingdom

There are currently ten agencies formally involved in intelligence in the UK.[17] We searched the public archives of five UK oversight organizations ([39]..[45]). The Intelligence and Security Committee of Parliament (ISC; http://isc.independent.gov.uk); the Investigatory Powers Tribunal (IPT; http://www.ipt-uk.com); Interception of Communications Commissioner's Office (IOCCO; http://iocco-uk.info); The Intelligence Services Commissioner's Office (http://intelligencecommissioner.com) and the Office of Surveillance Commissioner's (OSC; https://osc.independent.gov.uk). The studied archives of the ISC do not refer to any security consequences of the Snowden files. The archives of the IPT mention the increase of workload caused by the Snowden incidents, the opinion that the UK legislation has failed to keep abreast of the consequences of technology advances and the conclusion that '*the Snowden revelations in particular have led to the impression voiced in some quarters that the law in some way permits the Intelligence Services carte blanche to do what they will. We* [the IPT] *are satisfied that this is not the case*' (IPT, Additional Report 2011-2015, p.26, [43]). The archives of the IOCCO [42] do not mention any security consequences of the Snowden files. However, they contain an interesting reference to the dogmata of secrecy: '*They* [the secrecy regulations] *mean that I am not able to confirm or reject publicly parts of the detail said to derive from Snowden allegations. A reader should not draw any inference one way or the other in this respect from what I do say. However, as will I trust appear, I am able to address matters of concern in a way which I hope will be helpful*' (IOCCO, Annual Report 2013, p.40, [42]). The archives of the Intelligence Services Commissioner's Office and of the OSC also do not mention any security consequences. It is apparent that the main concern of all of these oversight organizations is the alleged abuse of powers by intelligence agencies and not the alleged security consequences of the Snowden files. This is in sharp contrast with the public position taken by the government.

3.4.3. The Netherlands

The Dutch General Intelligence and Security Service (GISS)[18] and Defence Intelligence and Security Service (DISS)[19] are supervised by The Commission on the Intelligence and Security Services ('CIVD'; https://-www.houseofrepresentatives.nl/members_of_parliament/-committees/iv), a committee of the Dutch House of Representatives and by The Commission for Supervision of Intelligence and Security Services ('CTIVD'; http://-english.ctivd.nl), a government committee composed of independent intelligence experts. We included the available Annual Reports of the GISS [48] and the DISS [47], all of the communications of the House of Representatives and Senate mentioning Snowden (https:-//www.houseofrepresentatives.nl and https://www.eerste-kamer.nl/begrip/english_2) and the Annual Reports, press releases and Supervisory Reports of the CTVID ([52]..[54]) and the Annual Reports[20] of the CVID [46] in our research. The National Coordinator for Counterterrorism and Security ('NCTV'; https://english.-nctv.nl) is a government official and office that coordinates all intelligence. The public communications of this office were also included in our research ([49]..[51]). None of these sources assert that a relation exists between the Snowden files and diminishing security, let alone that facts are presented that corroborate such a relation.[21]

4. Conclusions and Further Research

It is tempting to conclude that the publication of the Snowden files has clear consequences. A number of documented media publications, for example about Prism and the concerted public statements of governments about negative consequences for security, suggest this clarity. We must, however, realize that publications of documented examples of the (mis)behaviours of secret services do not generalize to the reliability of allegations of threats to security. The successful and founded media publications based on the Snowden files can influence

[16] It is of course possible that a belief creates a stronger conviction than actual perception or logical implication. Our preliminary interpretation is that Flynn is just honest.

[17] Security Service/MI5 (https://www.mi5.gov.uk); National Domestic Extremism and Disorder Intelligence Unit (NDEDIU; http://www.npcc.police.uk/NationalPolicing/NDEDIU/-AboutNDEDIU.aspx); National Crime Agency (NCA; http://nationalcrimeagency.gov.uk); National Ballistics Intelligence Service (NABIS; www.nabis.police.uk); National Fraud Intelligence Service; Secret Intelligence Service (SIS)/MI6 (www.sis.gov.uk); Defence Intelligence (DI; www.gov.uk-/government/groups/defence-intelligence#defence-intelligence); Government Communications Headquarters (GCHQ; www.-gchq.gov.uk); Joint Intelligence Organisation (JIO; www.gov.-uk/government/groups/joint-intelligence-organisation) and National Counter Terrorism Security Office (NaCTSO; www.gov.uk/government/organisations/national-counter-terrorism-security-office).

[18] https://english.aivd.nl.

[19] https://www.defensie.nl/organisatie/bestuursstaf/inhoud/een-heden/mivd.

[20] The Annual reports of 2015 and 2016 are not yet available to date.

[21] The other side of the revelation of the Snowden files is confirmed explicitly. The 'CTIVD' concluded that the GISS unlawfully exchanged 1.8 million satellite phone metadata with the NSA. A fact that was revealed by the Snowden files. (CTVID Supervisory Report 38, 2014, February 5, [54]). The required permission of the Secretary of Justice was missing, i.e. there was no executive or congressional oversight.

public opinion in a twisted way. Sensitive information has obviously been leaked and has hurt sensitive interests, i.e. our confidence in our secret services, therefore the general proposition that this information hurts other sensitive interests, like security interests, gets more credibility. This generalization could be justified. However, the available facts do not justify it at this moment.

Our preliminary research as described above suggests that there are insufficient facts to draw any founded conclusions about the possible consequences of the Snowden files for security. The Snowden files are hardly available. What is available has been selected to corroborate the media publications mentioned. Data about actual security consequences are not available. Our search of the intelligence archives of the USA, the UK and the Netherlands suggests that these data are not only unavailable, but absent. The dogmata of secrecy prescribe that classified information is not published and that we trust in our governmental and parliamentary oversight organizations and their public accounts. However, if these organizations even fail to report in an abstract or generalized way that actually leaked facts have caused actual consequences that are harmful to security, then one should have doubts about their existence. What we found in the intelligence archives are repeated warnings and restatements of the theoretical consequences: 'if classified information is leaked, harm to security will be done' and 'leaking classified information does harm to security', which can be interpreted both as hypothetical and as factual statements. We are puzzled by this consequent choice for ambivalence in de formulations, but we demonstrate in this research that the methodology we chose can be effective. Further research is necessary. First, the obstacle of the unavailability of the Snowden files must be removed. It is understandable that journalists want to monopolize access to protect their sources, themselves or their scoops. However, the argument that publication should be done carefully and in context and that certain journalists are best equipped to do this leads to an elitist form of historicism and excludes other approaches to the material. There should be no problem in giving science access to all the Snowden files which are currently available to journalists under the condition that journalists hold on to all the concrete scoops and science concentrates on eliciting general knowledge. Science is for example not interested in publishing about Prism as such but it is interested in publishing about the failing oversight system and about the quality of the ratio for new legislation and the introduction of new executive powers. Secondly, oversight organizations, in particular those who serve representatives of the people, should be more careful to report clear abstracted accounts of classified information to provide the rationale for the new legislation and powers which are necessary to adapt to the changed reality of transparency. Finally, government officials and former government officials should be more careful about their statements regarding the consequences of the leaks of classified information. The best illustration of this is the alleged relation between the Snowden files and the use of cryptography by the terrorists involved in the Paris attacks. A first look at the underlying facts seems not to be supportive of this opinion.

So we will try to establish scientific cooperation and cooperation with journalists. We will try to inform oversight organizations and we will do further research testing the technical backgrounds of political allegations. As long as the dogmata of secrecy prevail, the blind will be leading the sheep.

Acknowledgements

N.F.W. Sturris and I. de Groot (LLB students) have participated in the media and literature research.

References

A complete list of studied sources will be made available for further research.

Snowden Files

[1] American Civil Liberties Union (ACLU). *NSA Documents*. Retrieved from https://www.aclu.org/nsa-documents-search (776 documents) and https://www.aclu.org/nsa-documents-released-public-june-2013.

[2] Canadian Journalists for Free Expression (2016, August 19). *Snowden Surveillance Archive*. Retrieved from https://snowdenarchive.cjfe.org (1182 documents).

[3] Courage Foundation & Transparency Toolkit. *Snowden Document Search*. Retrieved from https://search.edwardsnowden.com (748 documents).

[4] Cryptome (2013, September 7). *Snowden Tally*. Retrieved from https://cryptome.org/2013/11/snowden-tally.htm.

[5] Electronic Frontier Foundation (EFF). *NSA Primary Sources*. Retrieved from https://www.eff.org/nsa-spying/nsadocs.

[6] NSA Observer. *Documents*. Retrieved from https://github.com/nsa-observer/documents/tree/master/files/pdf.

[7] The Intercept (2016, August 10). *Snowden Archive. The SIDtoday Files.* Retrieved from https://theintercept.com/snowden-sidtoday/.

Public Media

[8] De Telegraaf (2013-2016). Retrieved from www.telegraaf.nl.

[9] Der Spiegel (2013-2016). Retrieved from www.spiegel.de.

[10] The Guardian (2013-2016). Retrieved from www.theguardian.com.

[11] The Intercept (2013-2016). Retrieved from www.theintercept.com.

[12] The Sun (2016). Retrieved from https://www.thesun.co.uk.

[13] The Washington Post (2013-2016). Retrieved from www.washingtonpost.com.

[14] USA Today (2013-2016). Retrieved from www.usatoday.com.

Literature (selection out of 215 consulted sources)

[15] Al-Qaeda in the Arabian Peninsula (2010-2013). *Inspire Magazine*. Al-Malahem Media. Retrieved from https://publicintelligence.net/?s=inspire.

[16] Berghel, H. (2014). Mr. Snowden's legacy. *Computer*, *47*(4), pp. 66-70.

[17] Bochel, H., Defty, A., & Kirkpatrick, J. (2014). *Watching the watchers: parliament and the intelligence services.* Houndmills: Palgrave Macmillan.

[18] Castro, D., & McQuinn, A. (2015). Beyond the USA Freedom Act: How U.S. Surveillance Still Subverts U.S. Competitiveness. *ITIF*, pp. 1-11. Retrieved from https://itif.org.

[19] Clark, R.A. et al (2013). *Liberty and Security in a Changing World. Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies.* Retrieved from www.whitehouse.gov.

[20] European Parliament (2013). Resolution on the US National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' privacy (2013/2682(RSP)). Retrieved from http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2013-0322&language=EN.

[21] Fenster, M. (2012). Disclosure's effects: WikiLeaks and transparency. *Iowa Law Review*, *97*(3), pp. 753–807.

[22] Flashpoint Global Partners (2014). *Measuring the Impact of the Snowden Leaks on the Use of Encryption by Online Jihadists.* Retrieved from https://fpjintel.com/public-reports/measuring-the-impact-of-the-snowden-leaks-on-the-use-of-encryption-by-online-jihadists/.

[23] Goldman, Z.K., & S.J. Rascoff (2016). *Global intelligence oversight: governing security in the twenty-first century*. New York: Oxford University Press.

[24] Harding, L. (2014). *The Snowden Files. The inside story of the world's most wanted man*. London: Guardian Books.

[25] Recorded Future (2014). How Al-Qaeda Uses Encryption Post-Snowden Part 1 and Part 2. *The Recorded Future Blog*. Retrieved from https://www.recordedfuture.com/al-qaeda-encryption-technology-part-1/.

[26] Richelson, J.T. (2013). The Snowden Affair. Web Resource Documents the Latest Firestorm over the National Security Agency. *National Security Archive Electronic Briefing Book*, no. 436. Retrieved from http://nsarchive.gwu.edu/NSAEBB/NSAEBB436.

[27] Shafer, J. (2014). Live and Let Leak State Secrets in the Snowden Era. *Foreign Affairs New York*, *93*(2), pp.136-142.

[28] United Nations Office on Drugs and Crime (2012). *The use of the Internet for terrorist purposes*. New York: United Nations. Retrieved from https://www.unodc.org.

[29] Verkaik, R. (2015, January 20). Al Qaeda's YouTube guide for jihadists: Security chiefs spooked over terror video that proves extremists are using leaks from US spy Edward Snowden to evade justice. *Daily Mail Online*. Retrieved from www.dailymail.co.uk.

[30] de Vey Mestdagh, C.N.J. (2015). De vijf dogma's van de geheimhoudingsreligie of in welk kabouterland zijn wij nu toch verzeild geraakt? (The five dogmata of the global religion of secrecy or in what nation of gnomes have we gone astray?). *Tijdschrift voor Internetrecht*, (4), pp. 148-152.

Intelligence Archives

United States of America

[31] House of Representatives, USA. *Annual reports*: 113-310; 113-714; 113-717. Retrieved from http://fas.org/irp/congress and https://www.congress.gov.

[32] House of Representatives, USA. *Reports*: 113-39; 113-102; 113-155; 113-277; 113-314; 113-446; 113-452; 113-463; 113-682; 113-719; 114-109 Part 1; 114-321; Majority Staff Report (2013, July 31); The Road to Boston: Counterterrorism Challenges and Lessons from Marathon Bombings (2014); Executive Summary of Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden (2016, September 15). Retrieved from http://fas.org/irp/congress, https://www.congress.gov and https://intelligence.house.gov.

[33] House of Representatives, USA (2013, October 29). *Testimonies before the Permanent Select Committee on Intelligence*: Baker, S.A.; Bradbury, S.G. Retrieved from http://intelligence.house.gov.

[34] House of Representatives, USA. *Transcripts of Permanent Select Committee on Intelligence Business Meetings*: 2014, February 10; 2014, March 6; 2014, March 13; 2014, May 29; 2014, July 24. Retrieved from https://intelligence.house.gov.

[35] Senate, USA. *Hearings*: 113-89; 113-600; Statement of Prioletti, B.A. (2013, October 31). Retrieved from http://www.intelligence.senate.gov/hearings and http://www.senate.gov.

[36] Senate, USA. *Preliminary Hearings of the Homeland Security and Governmental Affairs Subcommittee on the Efficiency and Effectiveness of Federal Programs and the Federal Workforce and Subcommittee on Financial and Contracting*

Oversight: 2013, June 20; 2013, November 19; 2013, November 20. Retrieved from http://www.senate.gov.

[37] Senate, USA. *Reports*: 113-7; 113-34; 113-81; 113-111; 113-118; 113-119; 113-120; 113-176; 113-195; 113-218; 113-233; 113-257; 113-276; 113-283; 113-287; 113-288; 113-323; 114-8; 114-33; 114-79; 114-178; 114-246; 114-297; Majority Staff Report of the Permanent Subcommittee on Investigations (2014, August 28); Review of the Terrorist Attacks on U.S. Facilities in Benghazi, Libya (2014, November 21). Retrieved from http://fas.org/irp/congress, https://www.congress.gov and http://www.senate.gov.

[38] Senate, USA. *Testimonies before the Committee on Homeland Security and Governmental Affairs*: Canterbury, A. (2013, November 20); Niehaus, P.J. (2015, May 20); Nojeim, G.T. (2015, January 28); Stern, J. (2016, January 20). Retrieved from http://www.senate.gov.

United Kingdom

[39] Intelligence and Security Committee of Parliament (ISC), UK. *Annual reports*: 2012-2013; 2013-2014; 2015-2016. Retrieved from http://isc.independent.gov.uk/committee-reports/annual-reports.

[40] Intelligence and Security Committee of Parliament (ISC), UK. *Special reports*: Report on Foreign Involvement in the Critical National Infrastructure (2013); Statement by the ISC regarding GCHQ's alleged access to the US PRISM programme (2013); Privacy and Security: A modern and transparent legal framework (2015). Retrieved from http://isc.independent.gov.uk/committee-reports/special-reports.

[41] Intelligence Services Commissioner's Office, UK. *Annual reports*: 2013; 2014; 2015. Retrieved from http://intelligencecommissioner.com/content.asp?id=19.

[42] Interception Of Communications Commissioner's Office (IOCCO), UK. *Annual reports*: 2013; 2014; 2015. Retrieved from http://iocco-uk.info/sections.asp?sectionID=1&type=top.

[43] Investigatory Powers Tribunal (IPT), UK. *Additional report 2011-2015*. Retrieved from http://www.ipt-uk.com/content.asp?id=33.

[44] National Crime Agency (NCA), UK. *Annual reports*: 2013-2014; 2014-2015; 2015-2016. Retrieved from http://nationalcrimeagency.gov.uk.

[45] Office of Surveillance Commissioners (OSC), UK. *Annual Reports*: 2013-2014; 2014-2015; 2015-2016. Retrieved from https://osc.independent.gov.uk/about-us/annual-reports-2.

The Netherlands

[46] Committee on the Intelligence and Security Services (CIVD), The Netherlands. *Annual reports*: 2013; 2014. Retrieved from www.officielebekendmakingen.nl.

[47] Defence Intelligence and Security Service (DISS), The Netherlands. *Annual reports*: 2013; 2014; 2015. Retrieved from https://www.rijksoverheid.nl.

[48] General Intelligence and Security Service (GISS), The Netherlands. *Annual reports*: 2013; 2014; 2015. Retrieved from https://www.aivd.nl.

[49] National Coordinator for Security and Counterterrorism (NCTV), The Netherlands. *Cyber Security Assessment Netherlands (CSAN)*: 2013; 2014; 2015. Retrieved from https://www.ncsc.nl/actueel/Cybersecuritybeeld%2BNederland.

[50] National Coordinator for Security and Counterterrorism (NCTV), The Netherlands. *Magazine Nationale Veiligheid en Crisisbeheersing (Magazine for National Security and Crisis Management)*: 2013(3) – 2016(3). Retrieved from https://www.nctv.nl.

[51] National Coordinator for Security and Counterterrorism (NCTV), The Netherlands. *Nieuwsbrief Nationaal Crisiscentrum (Newsletter National Crisis Centre)*: 2013, August - 2016, June. Retrieved from https://www.nctv.nl.

[52] Review Committee on the Intelligence and Security Services (CTIVD), The Netherlands. *Annual reports*: 2013; 2014; 2015; 2016. Retrieved from www.ctivd.nl.

[53] Review Committee on the Intelligence and Security Services (CTIVD), The Netherlands. *Press releases*: 2013-2016. Retrieved from www.ctivd.nl.

[54] Review Committee on the Intelligence and Security Services (CTIVD), The Netherlands. *Supervisory reports*: 22b; 37; 38, 39; 42; 47; 48; 49. Retrieved from www.ctivd.nl.