Intelligence Threats, Triumphs and Blunders:

How Damaging are Unauthorised Disclosures to National Security?

[NAME]

(Edited and or reviewed by Microsoft Software)

2401049

BA (Hons) – Security, Intelligence and Cyber

The University of Buckingham (2024-2026)

[Author's Notes: https://archive.org/details/2401049-Dec2024-01]

Table of Contents

Introduction.

Unauthorised disclosures of classified information have become a significant concern in the modern age of security studies. With an increase in national surveillance and technical and cyber security concerns, alongside a wave of modern anarchism and open-state theorists – the decision to leak classified information has far-reaching and complex consequences. From heralding those who disclose as saints to brandishing them as traitors, the modern populace has a varying degree of support to these people. Furthermore, these disclosers typically start conversations regarding government overreach, privacy and public accountability and it is for that reasons that it can be argued that these disclosures, while often bring uncalculated harm, can serve a public good. It is the aim of the essay to explore how damaging unauthorised disclosures are to national security.

While it is easy to say that unauthorised disclosures are damaging to national security, it is necessary to seek out case studies to explore the extent to which these disclosures present risk. The case studies to explore within this essay are three examples where sensitive and classified information has been released to the public via incorrect channels, resulting in various levels of fallout – namely The Snowden incident, Project Azorian and Operation Rubicon. These are three key examples of how fragile national (and international for that matter) security can be, they give a much-needed insight into the diverse nature of the consequences and risk that these disclosures pose, offering a nuanced understanding of the ethical and strategic implications, especially when one considers the argument that unauthorised disclosure of information can pose risks, but in some circumstances is necessary to uphold law and order within a nation, to uphold intelligence agencies to the same principles they are created to protect.

Case Study 1: Edward Snowden.

Edward Snowden, a former NSA (National Security Agency [USA]) Contractor and infamous 'whistleblower', became widely known in 2013 when he leaked millions of classified documents, including NSA files relating to global surveillance programs – most notably PRISM and XKeyscore. PRISM, the program whereby the NSA demanded information regarding NON-US persons, from IT companies under the FISA (Foreign Intelligence Surveillance Act) amendments act. Section 702 of the Amendments Act (2008) "permits the [Federal] government [of the United States] to conduct targeted surveillance of foreign persons located outside the United States, with the compelled assistance of electronic communication service providers, to acquire foreign intelligence information"[1]. XKeyscore, on the other hand, is the computer system that the NSA uses to search and analyse digital data globally, in real time. XKeyscore has proven to be a controversial and yet incomprehensibly useful tool for the protection of national interests of the United States, The NSA – in a press statement in 2013 – has confirmed how powerful XKeyscore has been to the US, "as of 2008, there were over 300 terrorists captured using intelligence generated from XKEYSCORE."[2] This indicates that while XKeyscore has numerous ethical concerns, officially the benefit to the national security of the US outweighs the cost of personal privacy.

Edward Snowden's motivations for leaking classified were based in his belief that the NSA had crossed the line, and their actions were in direct violation of the rights of privacy for

[1] Office of the Director of National Intelligence (n.d.). *Section 702 Overview*. [online] www.dni.gov. Available at: https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf [Accessed 28 Nov. 2024].

[2] National Security Agency (2013). *Press Statement on 30 July 2013*. [online] National Security Agency/Central Security Service. Available at: https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/1620989/press-statement-on-30-july-2013/ [Accessed 30 Nov. 2024].

the “targets”. His leaks exposed how surveillance programs operated with limited oversight, often targeting ordinary and innocent citizens not just the legitimate security threats. For example, the documents revealed that US allies, including Germany and Brazil, were subject to surveillance, straining the diplomatic ties and sparking international outrage globally.

The ramifications of Snowden’s actions were both immediate and enduring. Domestically, the US intelligence community faced operational setbacks as adversaries altered their communication methods to evade detection. The exposure of classified methods and tools compromised ongoing and future intelligence efforts, necessitating costly adjustments. On the global stage, Snowden’s leaks catalysed debates on privacy and the ethical boundaries of surveillance, leading to legislature reforms within the US – Such as the 2015 Freedom Act, which curtailed the bulk collection of phone metadata[3]. However, Snowden’s disclosures also attracted criticism for their perceived recklessness. By releasing vast amounts of classified data, he risked exposing sources, methods and operational plans – potentially endangering the lives of agents and assets around the world. Nonetheless, supporters of Snowden maintain that his revelations were a necessary catalyst for reform, highlighting the ethical dilemmas faced by intelligence agencies in balancing security with civil liberties.

[3] Orlando, M. (2019). *Reauthorizing the USA Freedom Act of 2015 | Federal Bureau of Investigation*. [online] Federal Bureau of Investigation. Available at: https://www.fbi.gov/news/testimony/reauthorizing-the-usa-freedom-act-of-2015-110619 [Accessed 1 Dec. 2024].

Case Study 2: Project Azorian.

Project Azorian was a covert CIA operation launched in the 1970s to recover the remains of the Golf II class submarine, K-129. K-129 was a diesel-electric Ballistic missile Submarine, carrying an armament of R-21 (nuclear) missiles. Project Azorian (Also referred to as Operation Jennifer) was the United States attempt to find and locate the Sunken K-129 and retrieve its armament for analysis. The operation involved the construction of the Hughes Glomar explorer, a Speciality built deep sea drill ship, used under the guise of deep-sea mining. The ambitious effort, which cost the CIA roughly $800 million USD, also aimed to retrieve cryptographic material and other sensitive assets that would give an insight into the Soviet Union's military technology.

The cold war brought up issues of nuclear attack, thus securing a soviet nuclear warhead would greatly increase the American advance. This was a view shared by many members of the leading class. Markus Wolf, a notorious east German spy and former head of the foreign intelligence division of statsi, would later state in his memoir "Carter's presidency had created great concern in the kremlin, because he had presented a defence budget of more than $157 million, which he invested in the MX and Trident missiles and nuclear Submarines."[4] This fear was well founded as "One of the top soviet nuclear strategists confided to me that the recourses of our allies were not sufficient to match this"[5]

[4] Fischer, B. (1997). *A Cold War Conundrum: The 1983 Soviet War Scare*. [online] CIA Reading Room. Available at: https://www.cia.gov/readingroom/docs/19970901.pdf [Accessed 1 Dec. 2024].

[5] Markus Wolf, spionage chef im geheimen Kneg ennerungen (Dusseldorf and Munich List Verlag,1997), pp 326, 330-331

The exposure of project Azorian, in 1975 by investigative journalists, underscores the challenges against the state posed by unauthorised disclosures. While the operation was highly classified, its exposure had a surprising, limited impact of US intelligence capabilities or National Security – The minimal fallout may be attributed to the operation's partial failure, which was due to mechanical issues in the recovery of the submarine, causing half of the K-129 to fall apart, thus reducing the possible strategic value of theoretical assets. However, from an operational standpoint, Project Azorian was not a complete failure, the CIA managed to retrieve two nuclear torpedoes. Furthermore, the Ships bell was retrieved and given back to the Soviet Union to increase diplomatic ties between the two global powers.

Jack Anderson, the Pulitzer Prize winning journalist who also helped to reveal the history of the CIA's assassination plots against Fidel Castro[6], released the story under the notion that the sunken sub contained no true intelligence and thus was "a waste of the taxpayer's money"[7] however it can be argued that this perspective ignores the broader implications of the operation. Even though the operation did not go fully as planned, the operation proved how American ambition, and covert action can lead to securing key information. This can be seen through an extract of the journal 'Intelligence and National Security', "Yet the wreckage held secrets that promised to help the United States win the underwater Cold War, a hidden but important battleground in which each superpower raced to

[6] Anderson, J. (1979). *Plot Disclosure made CIA Squirm*. [online] CIA Reading Room. Available at: https://www.cia.gov/readingroom/docs/CIA-RDP88-01315R000300510003-3.pdf [Accessed 1 Dec. 2024].

[7] Center for the Study of Intelligence. (2012). *Studies in Intelligence Vol. 56, No. 1*. [online] *Defence Technical Information Center.*, p.38. Available at: https://apps.dtic.mil/sti/pdfs/ADA585911.pdf [Accessed 1 Dec. 2024].

develop countermeasures against the ever quieter, ever deadlier fleets of submarines deployed by the other."[8]

Ethically, Project Azorian raises critical questions about the balance between secrecy and accountability. While the public has a right to scrutinise government actions, especially those involving significant expenditures, the exposure of sensitive operations can erode the trust between the public and the intelligence agencies, regardless of if that trust is warranted or not. In this example, the unauthorised disclosure of project Azorian had little to no serious or irreversible damage to national security, instead it may have only weakened the credibility of the American intelligence institutions and cause slight embarrassment towards the leadership of the US Armed Force's with regards to their inability to secure sunken submarines.

[8] Bennett, M. T. (2017) 'Détente in deep water: the CIA mission to salvage a sunken Soviet submarine and US-USSR relations, 1968–1975', *Intelligence and National Security*, 33(2), pp. 196–210. doi: 10.1080/02684527.2017.1342344.

Case Study 3: Operation Rubicon.

Operation Rubicon stands out as one of the most audacious and intricate intelligence operations of the Cold War era, in fact it is often regarded as the sole most successful[9] intelligence operation in contemporary history. It was a covert collaboration between the United States' Central Intelligence Agency (CIA) and Germany's Bundesnachrichtendienst (BND). The operation revolved around the manipulation of encryption devices (Most notably the CX-52) manufactured by Crypto AG; a Swiss-based company renowned for its expertise in secure communication technologies. At its height, Crypto AG was trusted by over 100 states worldwide, including both allies and adversaries, making it an unparalleled gateway for intelligence collection. For example, in the report of visit to Crypto AG (Hagelin) by William F. Friedman, Special Assistant to the Director NSA, there is substantial evidence to suggest that the NSA were taking advantage of the Dutch (as early as 1955) with the use of the C-class cryptography devices, "I wish to point out, however, that the rehabilitation of the C-446 tools offers certain advantages to UKUSA; for once these tools have been rehabilitated, Hagelin will be able to make more C-446's than are needed by the Dutch."[10]

By engineering vulnerabilities into these machines, the CIA and BND gained the ability to intercept, decrypt, and analyse the supposedly 'secure' communications of numerous nations. This unprecedented access allowed them to monitor diplomatic and

[9] Dobson, M., Dymydiuk, J. and Mainwaring, S. (n.d.). *Operation Rubicon: the most successful intelligence heist of the 20th Century*. [online] warwick.ac.uk. Available at: https://warwick.ac.uk/newsandevents/knowledgecentre/society/politics/operation_rubicon/ [Accessed 1 Dec. 2024].

[10] Friedman, W. (1955). *report of visit to Crypto AG (Hagelin) by William F. Friedman, Special Assistant to the Director NSA.* [online] Available at: https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/friedman-documents/correspondence/FOLDER_117/41772899081198.pdf [Accessed 1 Dec. 2024].

military communications globally, providing invaluable intelligence that influenced Cold War strategies and decisions. However, the success of the operation relied on an extraordinary level of secrecy and the compartmentalization of information within Crypto AG itself, with only a small inner circle aware of the company's true role as a covert partner in intelligence gathering.

The secrecy of the operation began to fall apart in 1992 when Hans Bühler, a prominent sales representative for Crypto AG, was arrested in Iran. Bühler, a “highly valued”[11] employee, was not privy to the operation and was genuinely unaware of the covert activities involving the company's products, of which he worked with. Accused of espionage, Bühler endured 10 months of detention and intense interrogation. During this period, he grew increasingly suspicious of Crypto AG’s operations, speculating that the machines he had sold may have been compromised. His detention and subsequent allegations drew attention to the integrity of the company and set off a chain reaction that eventually exposed Operation Rubicon. Bühler spent years investigating the actions of Crypto AG and the involvements of the CIA and the BND, he complied these findings in his book “Verschlüsselt: der Fall Hans Bühler”[12] In 2018, Crypto AG was acquired by Crypto International AG, focusing “solely on supporting existing customers and their installations.” [13]

The fallout from this revelation was seismic. Nations that had depended on Crypto AG for secure communications felt deeply betrayed, viewing the manipulation of encryption

[11] Crypto Museum (2016). *Hans Bühler*. [online] www.cryptomuseum.com. Available at: https://www.cryptomuseum.com/people/buehler/hans.htm [Accessed 1 Dec. 2024].

[12] Bühler, H. (2018). *Verschlüsselt: der Fall Hans Bühler*. [online] Zürich : Werd-Verl. Available at: https://archive.org/details/verschlusseltder00stre/page/n3/mode/2up [Accessed 1 Dec. 2024].

[13] Crypto International AG (2018). *About | crypto.ch*. [online] Crypto.ch. Available at: https://crypto.ch/en/about#offering [Accessed 1 Dec. 2024].

devices as an unforgivable breach of trust. Many governments undertook urgent efforts to overhaul their communication infrastructures, fearing further exploitation by intelligence agencies. The exposure also damaged the reputations of the CIA and BND, casting a shadow over their relations with allies and partners. The operation was widely criticized as a violation of international trust and state sovereignty, sparking debates over the ethical boundaries of intelligence activities.

From an ethical standpoint, Operation Rubicon exemplifies the complex moral dilemmas inherent in intelligence work. On one hand, the operation yielded critical intelligence that likely shaped the geopolitical landscape of the Cold War, potentially averting conflicts or giving allied nations a strategic edge. On the other hand, the exposure of the operation highlighted significant ethical and human costs. Bühler's ordeal underscored the personal risks borne by individuals unknowingly entangled in covert activities, raising questions about the responsibility of intelligence agencies to safeguard their personnel.

Moreover, the operation's long-term impact on international relations cannot be understated. The betrayal experienced by many nations eroded trust in intelligence-sharing partnerships, casting a pall over cooperative security arrangements. The incident also prompted broader conversations about the ethical limits of statecraft, particularly in balancing national security interests against the principles of transparency and sovereignty.

Conclusion.

The unauthorised disclosure of classified information undeniably poses a binary threat to national security but what degree of damage this threat to national security possesses can be in relation to the nature of the threat itself. This is seen throughout the case studies I have examined. The Snowden incident sparked vital debates about privacy and surveillance globally, but also caused significant operational disruptions and diplomatic collateral damage. To contrast this, Anderson's investigations into project Azorian demonstrated that not all exposures of classified material cause catastrophic consequences. While Anderson exposed operational details, these had no effect on the result of the operation and it could be argued that since the release of Anderson's findings, the intelligence community has been more transparent on their budgeting. Lastly, operation rubicon cements the ideology that the business of intelligence is a moral grey area thus ethical issues are a natural result of the environment in which the community operates.

The nature of the information, the motivations of the discloser and the subsequent reaction of those involved are key factors that play into the final verdict. While some disclosures ignite debates necessary for the evolution of society, others come at too great of a risk for those whose lives are deeply tied to the information released, as seen in the Snowden files. Ultimately, the balance between national security and the publics right to privacy and accountability remains precarious and is best modelled by the narrowest of lines. The complexity of these issues requires robust oversight and safeguarding mechanisms. As governments strive to protect their citizens, they must also question at what point it is too great of a cost to continue, and this rhetoric applies to those who wish to disclose intelligence - At what point does the cost outweigh the victory?

Reference List:

Anderson, J. (1979). *Plot Disclosure made CIA Squirm*. [online] CIA Reading Room. Available at: https://www.cia.gov/readingroom/docs/CIA-RDP88-01315R000300510003-3.pdf [Accessed 1 Dec. 2024].

Bennett, M. T. (2017) 'Détente in deep water: the CIA mission to salvage a sunken Soviet submarine and US-USSR relations, 1968–1975', *Intelligence and National Security*, 33(2), pp. 196–210. doi: 10.1080/02684527.2017.1342344.

Bühler, H. (2018). *Verschlüsselt: der Fall Hans Bühler*. [online] Zürich : Werd-Verl. Available at: https://archive.org/details/verschlusseltder00stre/page/n3/mode/2up [Accessed 1 Dec. 2024].

Center for the Study of Intelligence. (2012). *Studies in Intelligence Vol. 56, No. 1*. [online] *Defence Technical Information Center.*, p.38. Available at: https://apps.dtic.mil/sti/pdfs/ADA585911.pdf [Accessed 1 Dec. 2024].

Crypto International AG (2018). *About | crypto.ch*. [online] Crypto.ch. Available at: https://crypto.ch/en/about#offering [Accessed 1 Dec. 2024].

Crypto Museum (2016). *Hans Bühler*. [online] www.cryptomuseum.com. Available at: https://www.cryptomuseum.com/people/buehler/hans.htm [Accessed 1 Dec. 2024].

Dobson, M., Dymydiuk, J. and Mainwaring, S. (n.d.). *Operation Rubicon: the most successful intelligence heist of the 20th Century*. [online] warwick.ac.uk. Available at: https://warwick.ac.uk/newsandevents/knowledgecentre/society/politics/operation_rubicon/ [Accessed 1 Dec. 2024].

Fischer, B. (1997). *A Cold War Conundrum: The 1983 Soviet War Scare*. [online] CIA Reading Room. Available at: https://www.cia.gov/readingroom/docs/19970901.pdf [Accessed 1 Dec. 2024].

Friedman, W. (1955). *report of visit to Crypto AG (Hagelin) by William F. Friedman, Special Assistant to the Director NSA*. [online] Available at: https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/friedman-documents/correspondence/FOLDER_117/41772899081198.pdf [Accessed 1 Dec. 2024].

Markus Wolf, spionage chef im geheimen Kneg ennerungen (Dusseldorf and Munich List Verlag,1997), pp 326, 330-331

National Security Agency (2013). *Press Statement on 30 July 2013*. [online] National Security Agency/Central Security Service. Available at: https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/1620989/press-statement-on-30-july-2013/ [Accessed 30 Nov. 2024].

Office of the Director of National Intelligence (n.d.). *Section 702 Overview*. [online] www.dni.gov. Available at: https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf [Accessed 28 Nov. 2024].

Orlando, M. (2019). *Reauthorizing the USA Freedom Act of 2015 | Federal Bureau of Investigation*. [online] Federal Bureau of Investigation. Available at: https://www.fbi.gov/news/testimony/reauthorizing-the-usa-freedom-act-of-2015-110619 [Accessed 1 Dec. 2024].