Cyber Vigilante Individuals as Non-State Actors: Introducing Their Relevance to the Field of International Relations

Fitzpatrick, Nicolas

Cyber Vigilante Individuals as Non-State Actors

Introducing Their Relevance to the Field of International Relations

By Nicolas Fitzpatrick

Word Count: 14946

Table of Contents

1. Introduction

From Robin-Hood and Zorro to Batman and Spiderman, the idea of vigilantes as defenders of the common has been ubiquitous across societies. Vigilantes and vigilante groups have been present through history with a variety of motivations, but participation often included personal risks dissuading many. The 21st century brought with it an invention that would significantly lower these risks and lead to a surge in vigilantism that persists today - the internet.

Cyber Vigilantism, also referenced as 'netlantism' (Chang & Zhu, 2020), 'digital vigilantism' (Favarel-Garrigues et al., 2020), and 'Internet Vigilantism (Chang et al, 2018), has been of great recent interest for academics attempting to untangle the messy and problematic public sphere which is the internet. To provide context, a basic definition of cyber vigilantism can generally be seen as "Online actions in pursuit of what is seen as justice by self-appointed individuals or groups lacking legal authority." (Chandler & Munday, 2016).

This retaliation can be in many forms, from scambaiting, hacktivism, and crowdsourced investigations (Smallridge, 2016) to 'name and shame' campaigns and information leaking (Trottier, 2017). As such a varied phenomenon, cyber vigilantism has been studied through an equally varied lens, be it questions of ethics, its transformative effect on societal participation, its ramifications for legal systems, and as a citizen-led pursuit of social justice (Favarel-Garrigues et al., 2020). Regardless of the approach, what cannot be understated is the agency cyber vigilantism has granted individuals as empowered citizens to become self-appointed guardians of a particular social order (Favarel-Garrigues et al., 2020, p. 191).

Relatively new, cyber vigilantism has found relevance with scholars from backgrounds such as sociology, criminology, media studies, and anthropology (Favarel-Garrigues et al., 2020, p. 193). As such, its prominent engagements have focused on use by citizens for lateral surveillance - in other words how it has granted individuals agency to render other individuals the subject to their newfound digital power (Trottier, 2017, Loveluck, 2020).

While much has been written about cyber vigilantism in this regard, recent developments in the technology and tools available to cyber vigilantes have signaled cause for scholars of International Relations (IR) to take note. Certainly, the 200,000 strong IT Army of Ukraine - a group of volunteer hacktivists from across the world responsible for disabling Russian government websites, disrupting bank services, and DDoS attacks in Russian infrastructure

(Tidy, 2023) – would find that they have had an impact on the Russian state. Indeed, with the rise of what has been called the 'second generation of Open-Source Intelligence' (Williams & Blum, 2018), it is time to question whether cyber vigilantes have also found themselves agency in an international context.

It is from this position that this thesis begins its exploration. Specifically, this thesis seeks to determine: How can cyber vigilante individuals be justifiably included as non-state actors deserving of more attention within IR academia given the newfound transnational saliency of cyber vigilantism? This question requires two clarifying points. First, the use of saliency is in relation to the ability cyber vigilantism has to affect security at a state level. If the case is to be made that cyber vigilante individuals are worthy of study by scholars of IR, whether their impact on state security can be tangibly felt is a strong starting criterion. Second, the dimension of the 'individual' is especially important to this question. As will be demonstrated, there exists multiple cases of cyber vigilantism where individuals have worked alone to both positively and negatively affect state security. If individuals can be shown as having a degree of international saliency through cyber vigilantism, conceptions of valid NSAs by IR academia will be compelled to expand for their inclusion.

In approaching this question, this thesis will take a two-fold strategy. First, a two-block literature review will be employed as a methodology to serve distinct purposes. Block one will prove that there is an existing gap in IR literature on NSAs regarding both individuals and cyber vigilantism by outlining the rise and stagnation of NSA conceptions and then comparing literature on cyber vigilantism from other fields. Block two will utilize integrative literature review as outlined by Torraco (Torraco, 2005) to synthesize existing theoretical frameworks and create a slightly expanded theoretical framework of cyber vigilantism as '*producers of state security and insecurity*' to better incorporate its newfound transnational element. If cyber vigilante individuals are to be seen as salient NSAs, this expansion is necessary as it allows for a starting point in which cyber vigilantism can be introduced into IR literature for further development.

Second, this thesis will employ congruence analysis through two cases of transnational cyber vigilantism, testing the expanded theory against its synthesized predecessors. This will be done to not only demonstrate that this expanded theory is the 'best fit' as a framework that

incorporates cyber vigilantism into IR conceptions of NSAs, but also to highlight real-world instances where individual cyber vigilantes have had a salient impact on state security.

Ultimately, it will be found that given the lack of engagement from the IR community regarding cyber vigilantism and individuals as NSAs, the expanded framework of cyber vigilantism as 'producers of state security and insecurity' serves as an adequate starting point for its inclusion into IR academia. When paired with the cases explored, a case is made for further research into existing empirical cases and a meaningful integration of cyber vigilante individuals into IR canon.

The outline of this thesis is as follows. First, a section will examine the rise of the 'second generation' of OSINT (Williams & Blum, 2018), to highlight how it has given cyber vigilante individuals a transnational agency. Then, a brief methodology section will further break down the methodological tools used. Following, the two blocks of literature review will be worked through and followed by a congruence analysis of real-world cases and subsequent findings. Finally, this thesis will conclude with general thoughts on the question broached and suggestions for further research.

2. Background - The 'Second Generation of OSINT'.

Cyber vigilantism rose to prominence in academia in the early teens of the 21st century. Preliminary articles were descriptive in nature. Initial interest stemmed from vigilantism in Chinese cyberspace. DK Herold wrote in 2008 on the emergence of a civic society over the Chinese internet as social groups began to recognize their power and developed into internet vigilantes (Herold, 2008). Huang attributes a similar starting point in his work on internet vigilantism as a form of mediatized justice seeking in China from 2006-2018 (Huang, 2021). The first phenomenon identified was the Chinese Human Flesh Search Engine (HFSE), described as a: "form of online vigilante justice where Internet users hunt down and punish people…The goal is to get the targets of a search fired from their jobs, shamed in front of their neighbours, run out of town." (Downey, 2010, as cited in Gao & Stanyer, 2013, p. 2). Of particular interest were implications of collective action, justice and retribution, and political protest against corruption (Chang and Poon, 2017; Gao, 2016; Chang and Zhu, 2020; Gao & Stanyer, 2014).

One of the first times cyber vigilantism entered the public eye was the aftermath of the 2013 Boston Marathon Bombing. Described as a pivotal moment in citizen involvement in policing, members of a Reddit forum the 'Reddit Bureau of Investigation' engaged in cyber vigilantism by crowdsourcing investigative efforts to identify the bombers using media of the incident which killed three and injured 170 (Nhan et al., 2015). Their web sleuthing identified two suspects and started a witch-hunt that spread across the internet and news coverage, leading to the harassment of the suspects families (BBC, 2013). Ultimately, the cyber vigilantes had made a grave error in the identifications as both suspects were proven innocent. Here, cyber vigilantism was recognized as a tool that empowered citizens against corruption (as in the case of the HFSE) and as one that could bring with it damaging repercussions. (Nhan et al., 2015). As a direct result, questions around whether cyber vigilantism could be properly managed and 'reined in' by police forces began to arise (Nhan et al., 2015; Kosseff, 2015). Still, cyber vigilantism was primarily seen as a phenomenon which enabled citizen policing, particularly in a domestic environment.

A new shift in the digital technology available to citizens, however, has perhaps called for cyber vigilantism to be examined beyond its effect on the domestic realm and towards the international.

Dubbed the 'second generation of open-source intelligence (OSINT)' by the RAND Corporation (Williams & Blum, 2018), this shift came in tangent with the introduction of the 'Web 2.0' in which the internet transitioned to spaces of dynamic websites, user-led content generation, and social media ((Williams & Blum, 2018, p. 2). Most importantly, the internet has led to unprecedented interconnectedness across the globe allowing for emerging technologies, previously only available to governments, to reach the hands of individuals (Zegart, 2023). The tools and capabilities of this generation of open-source intelligence are tricky to succinctly summarize. Dr. Amy Zegart is perhaps the leading voice on open-source intelligence, having written about the topic extensively. She has described open-source intelligence as a: "[publicly available] grab-bag of capabilities at the 'frontier of the frontier'...like following events on twitter…mining anything that is publicly available…using commercial satellite imagery." (Zegart, 2023, as interviewed in Kurtz-Phelan, 2023). What is critical to Zegart, however, is that the 'playing field' between government intelligence agencies and the private sector has almost leveled – indeed recent technological innovations are now born in the private sector and dual-

use, meaning they are sold in the commercial and government sectors (Zegart, 2023). New technologies such as precise commercial satellite imagery and geolocation functionalities, facial recognition software, easily accessible artificial intelligence tools, and quantum computing are all available to cyber vigilantes. These technological advances have made states far more vulnerable than before: in cyberspace threats are no longer geographically bound to air, land, and sea but now come from anywhere, and *anyone* (Zegart, 2023). States must add a new element to their threat list: private citizens.

Zegart uses the successes of Bellingcat, an open source investigative and activist journalism network', as an example of the impact OSINT can have when harnessed by citizens (Zegart, 2021). While famously known for uncovering Russian involvement in the shooting down of Malaysia Airlines flight 17, it has also compiled evidence of chemical weapon use by the Syrian government, unmasked members of a Russian hit-team sent to assassinate a former Russian military officer living in the United Kingdom (Zegart, 2021).

Cyber vigilante individuals have also found success using OSINT. Two weeks after the US capitol riots on January 6th, 2021 – where thousands of Trump supporters stormed the US capitol buildings – a website appeared called 'Faces of the Riot', with the faces of 6,000 unique, isolated, and geotagged capitol rioters showcased in catalogue-style (Greenberg, 2021). The creator, an anonymous college student in the Washington D.C. area, used Tensor Flow (an open-source machine learning tool) and Dlib (facial recognition software) to sort, cluster, and remove duplicate faces from his database (Greenberg, 2021). As will be explored through the cases included in the subsequent congruence analysis, cyber vigilante individuals have been able to employ OSINT tools transnationally as well.

The 'second generation of OSINT' (Williams & Blum, 2018) has acted as a catalyst for this thesis – with tools and technology that has expanded cyber vigilantism towards an international context. With these new capabilities in mind, a strong case is made for the inclusion of cyber vigilante individuals as salient NSAs in IR academia.

3. Methodology

As discussed, the aim of this thesis is to determine whether cyber vigilantism, by granting individuals transnational saliency, justifies their inclusion as non-state actors deserving of more attention within IR academia. To answer this question, this thesis will harness two distinct methodological tools: a two-block literature review consisting of a 'traditional' background block as well as a methodologically rigorous block of integrative literature review (posited by Dr. Hannah Snyder (Snyder, 2019, p. 335), and the subsequent use of loose congruence analysis applied to real-world case studies. These two tools will work linearly; the two-block literature review will act as a supportive structure on which the expanded framework of cyber vigilantism proposed by this thesis can then be worked through congruence analysis. The following section will demonstrate how these methodological tools are employed, as well as provide the rationale behind their inclusion.

3.1 Two-Block Literature Review

Literature Review, in simple terms, can be defined as a summarization and evaluation of the existing body of academic research on a given topic (Knopf, 2006). It is an integral part of any research article, regardless of the field of study, as it demonstrates an attempt by the author to actively engage with and critique previous efforts by others with similar research interests. More importantly, it can help align and justify the motivations, research question, and hypotheses of a research project (Snyder, 2019). So, it is generally seen as a given that a literature review, in one form or another, will always be included in an academic article.

Less common, however, is the use of Literature Review as a methodological tool. But when applied with deliberate steps and rigor, a Literature Review can be particularly illuminating as a methodology. For example, Snyder finds that Literature Review is best suited to questions that aim to evaluate and validate a theory (often in comparison to other theories), to provide an overview of a research problem, or for theory development and expansion (Snyder, 2019, p. 334). Integrative literature review, a type of literature review useful in the synthesis, expansion, and reconceptualization of theoretical frameworks, has been chosen for this thesis.

3.1.1 Explanation of Two Literature Review Blocks

While Snyder believes there is significant reward in using integrative literature review in the expansion or creation of conceptual models or theory, she does advise caution as they can lack in rigor and full integration of the existing research on a topic in comparison to its other forms (Snyder, 2019). To alleviate these concerns, this thesis includes two blocks of literature review with distinct purposes.

Block one is composed of a more 'traditional' literature review through which the historical rise and stagnation of NSA conceptions in IR is reviewed before exploring literature on both individuals and cyber vigilantism outside the field of IR. Block two presents as an integrative literature review on three selected theoretical frameworks of cyber-vigilantism with a focus on arriving (through synthesis) at an expanded framework that recognizes cyber vigilantism's newfound transnational ability as 'producers of state security and insecurity'.

The result is a more balanced literature review that can set the stage for meaningful congruence analysis, conducted in the second half of the thesis.

As literature review is already a given prerequisite of academic articles, it is important to go into depth on how its use will differ in this thesis as a methodological tool. As stated above, it is important when using literature review as a methodology to be more deliberate with the steps and rigor taken. This deliberation can be achieved in two ways:

1. Clearly demonstrating the strategy used when choosing articles to review.
2. Developing a method that is replicable, meaning a reader can harness the method used to conduct a similar study (Snyder, 2019).

Because the choice has been made to include two blocks of literature review, each with a distinct purpose, the strategy and method used in both blocks will be explained separately.

3.1.2 In-depth Analysis: Block One of Literature Review

This block of literature review is a replacement of the 'traditional' literature review component of academic articles. Its purpose is to provide background that allows for the research question to be better approached and evaluated. As such, its utility is in identifying a research gap regarding the exclusion of both individuals as NSAs and cyber vigilantism as a phenomenon

in IR literature. The identification of a research gap is necessary to justify their inclusion when specifically contrasted against the literature revolving around NSA individuals and cyber vigilantism from other fields. This is accomplished by using the standard literature review approach of evaluation (Snyder, 2019) with an emphasis on the historical context of NSA literature within the field of IR.

Admittedly, this section of literature review will be 'loose' in terms of rigor given its contextual and 'traditional' nature. The subsequent integrative literature review is far more methodologically important and rigorous, so more space has been allowed to properly explain its use.

3.1.3 In-depth Analysis: Block Two of Literature Review

As described by Snyder, integrative literature review is differentiated by its aim to:

> "assess, critique, and synthesize the literature on a research topic in a way that enables new theoretical frameworks and perspectives to emerge…to expand on the theoretical foundation of the specific topic as it develops." (Synder, 2019, p. 335-336).

Especially important to note is that integrative literature review is well suited to analyze both firmly grounded and emerging topics. This comes largely as a result of the initial data collection process of, which prioritizes the intentional combination of insights and perspectives on a topic over a broad scan of all its existing literature (Snyder, 2019, p. 336) As a guide to this integrative literature review, this thesis will harness the steps as suggested by Dr. Richard Torraco to ensure adequate conduct and rigor. (Torraco, 2005).

It is first important to identify why an integrative literature review has been chosen as a methodology (Torraco, 2005). Again, the goal is to expand upon three theoretical explanations of cyber vigilantism to arrive at a synthesized and expanded framework that better incorporates transnational elements of cyber vigilantism. As a mature topic outside of IR, integrative literature review is well equipped to review, critique, and expand the knowledge base of a developing topic like cyber vigilantism. (Torraco, 2005, p. 2). A reconceptualization is necessary to demonstrate the international reach of cyber vigilante individuals and allow for introduction to the field of IR.

The structure of this integrative literature review is shaped by a 'guiding theory' – a theoretical orientation held by the author that differs or is not properly addressed by existing thought on the topic (Torraco, 2005, p. 4). For this integrative literature review, as well as the thesis itself, the guiding theory rests upon the notion that due to the 'second wave' of OSINT technology, cyber vigilante individuals have a newfound ability to have a transnational impact on security.

Three frameworks of cyber vigilantism (Trottier 2017; Smallridge et al., 2016; Chang et al., 2018) will be worked through and critiqued along the lines of this guiding theory. The three frameworks have been chosen for two reasons. First, they are among the most popular frameworks on cyber vigilantism, with Trottier (2017) being the most cited at 207 citations, followed by Chang et al. (2018) at 77 citations, and Smallridge et al. (2016) with 66 citations. Second, these theories offer a fantastic starting point upon which an expanded theory of cyber vigilantism can be built as they are codified (Smallridge et al., 2016), well researched (Trottier, 2017), and already recognize individual saliency regarding state security (Chang et al., 2018). These criteria for selection can be used as loose guidelines allowing for repeatability in subsequent integrative literature reviews on the topic.

Integrative literature review includes two steps: an initial critical analysis of the literature collected followed by a synthesis of the literature to produce a reconceptualization (Torraco, 2005, p. 7).

Synthesis is especially important, as it allows this integrative literature review to weigh the positives and negatives of each article to arrive at an alternative model or conceptual framework, essentially being new ways to think about a topic. (Torraco, 2005, p. 8). Once this synthesis is completed, it will be possible to take this expansion and use congruence analysis to test against predecessors through real-world cases.

3.2 Congruence Analysis and Case Studies

Congruence analysis is primarily used to compare the strength of evidence available for different theoretical frameworks (Wauters and Beach, 2018, p. 20). As opposed to process tracing, congruence analysis does not require detail regarding causal mechanisms to concretely answer how 'X leads to Y', but instead takes the approach of evaluating which theoretical

framework can best explain how the outcome Y is arrived at. (Wauters and Beach, 2018, p. 19-20). It is best used in situations where there is an absence of a counterfactual, meaning that it is used not to indicate the 'correct' theoretical approach but instead establish comparative strength (Wauters and Beach, 2018, p. 20). Specifically, this article utilizes a 'competing theory approach' to congruence analysis, in which an evaluation of several theories across a range of cases is completed to find the 'best fit' (Wauters and Beach, 2018, p. 20).

The general steps to a competing theory approach of congruence analysis utilized by this thesis are taken from Blatter and Haverland, laid out structurally by Wauters and Beach (Blatter and Haverland, 2012, p. 163-164, as cited in Wauters and Beach, 2018). They are as follows:

1. Selection of broad theories and cases of interest. In this instance, the selection of theories is conducted in the integrative literature review. The selection of cases will be justified below.
2. Elaboration of hypotheses of each theory to showcase how factors in a case should play out if a given theory is valid.
3. These hypotheses and their theoretical backing are then tested against the real-world cases to see if expected outcomes match with observable outcomes.
4. Finally, the relative strength of each theory is put against each other to determine if a 'best fit' can be found (Blatter and Haverland, 2012, p. 163-164, as cited in Wauters and Beach, 2018).

It is noted that, despite following these guidelines, this thesis will employ congruence analysis in a less stringent manner than is otherwise possible. An expanded framework of cyber vigilantism is proposed because it recognizes that newfound transnational capabilities arising from OSINT technology may not be adequately represented in previous conceptions. It introduces a possible avenue that IR scholars could use to begin the implementation of cyber vigilantism and individuals in the study of NSAs – its goal is not to be a finalized and refined framework but instead one which kickstarts new ways of approaching the topic. Its utility, then, is in planting the seed for the inclusion of cyber vigilante individuals into IR academia. Congruence analysis is used to the point where the relevance and necessity of the expanded framework can be adequately justified.

Regardless of its less stringent use, this congruence analysis incorporates a deductive approach working to strengthen the more inductive approach taken in previous sections. As

defended by David Blagden, it is not only acceptable but also potentially beneficial to 'square the circle' between inductive and deductive strategies to theory crafting in IR (Blagden, 2016). Inductive reasoning, when used to identify a 'starting point' in a theory, can gain a higher degree of rigor when an analytically deductive component is included that allows for attempts at generalizable causal explanations (Blagden, 2016, p. 210). Congruence analysis, then, gives a much-needed element of empirical testing in which this inductively reached theory can be tested against the empirical record to measure its strength (Blagden, 2016, p. 210). While this does act to create a more refined argument, it is conceded that this paper's congruence analysis is only able to include two empirical cases. However, as noted by Blagden, even if only to land on a variant of an existing theory, one of the many benefits of including an empirical element is that it allows for more cases to be identified and pursued for further research (Blagden, 2016, p. 210).

Furthermore, given that congruence analysis is used to propose a theoretical framework more suited as a starting point for the inclusion of cyber vigilante individuals into IR literature, it would be difficult to champion a single theory with significant causality. It is far more responsible to compare the strength of this expansion compared to its predecessor and other competing theories rather than to identify it as the sole explanatory causal mechanism.

3.2.1 Choice of Case Studies

The congruence analysis detailed above is done across two real-world instances of cyber vigilantism undertaken by individuals. First is the case of the North Korean 'Disco-ball' – in which an individual used a variety of OSINT tools to identify the location of a North Korean nuclear facility. The second is the 2020 Natanz Fire, a cyber vigilante incident in which two non-proliferation experts, working separately, were able to investigate an explosion on Iranian soil using OSINT tools and arrive at numerous controversial (and potentially insecuritizing) conclusions. The cases chosen represent instances where cyber vigilantism was employed transnationally, by individuals using OSINT tools as described in the preceding chapter, and in which state security was affected.

4. Two-Block Literature Review

4.1 Block One: The Rise and Stagnation of NSAs in International Relations Theory: How Cyber Vigilante Individuals Have Been Missed

The purpose of this literature block is to prove that individuals have largely been discounted in IR academia as salient NSAs. This will be done by demonstrating how and why NSA literature has risen and then stagnated as a topic within IR, and how this has worked to exclude the potential introduction of entities like cyber vigilante individuals. Then, literature from fields outside of IR such as cybersecurity, cyberwarfare, and international cyber law will highlight the increasing relevance of individuals in the cyber realm. Finally, a brief look at existing literature on cyber vigilantism will indicate that the topic has yet to be engaged from an IR perspective.

4.1.1 The Rise of NSAs in IR

Discussion of NSAs can be traced back in modern IR theory as early as the 1960's, where the ability of non-state bodies to influence foreign policy transnationally was formally recognized in the works of transnationalists. (Halliday, 2001). While its origins stemmed from state-centric critiques, the idea of the NSA in IR theory passed from hand to hand through the second half of the 20th century, garnering the attention of Marxists, right-wing conservatives, left-wing liberalists, and neoliberalists (Halliday, 2001, p. 24-25). The most prominent 'boom' in relevance, however, came with the end of the Cold War. For many, the fall of the Berlin Wall shifted the world from a bi-polar system towards a global order characterized by globalization, transnational governance, and a newfound fascination with everything non-state. Of course, this fascination was not unfounded - the end of the Cold War also signaled the end of numerous barriers to cross-border engagement, allowing for a proliferation in the number of non-state actors such as INGOs, NGOs, and IGOs (Weiss et al., 2013). Scholars such as Weiss et al. accurately represent the logic behind much of the interest in this 'boom' with their finding: "more is different." (Weiss et al, 2013, p. 8).

The introduction of NSAs to the forefront of IR discussion led to the development of new theories and beliefs. Robert Keohane and Joseph Nye, for example, put forward a theory of 'complex interdependence' to explain a more intertwined global political economy (Keohane and Nye, 1989, as cited in Ataman, 2003). Most crucial, and in many ways controversial, was the conclusion arrived at by many IR experts that states are declining in power and importance, giving way to its new predecessor, the non-state actor (Ataman, 2003).

This belief has survived well into the 21st century. Josselin and Wallace, in conceptualizing a framework of NSAs, argued that any starting point of IR must consider the significance of NSAs on global politics; only the staunchest of realists would deny that NSA's have shifted the balance of power away from states (Josselin and Wallace, 2003., p. 1). Ataman, too, found that it is difficult to approach international relations and nation-states without acknowledging the great importance that non-state actors have on them, going as far as to say that all new theoretical and conceptual frameworks of IR must include non-state actors for a proper analysis (Ataman, 2003, p. 62)

The boom felt by NSAs through the late 20th and into the 21st century brought with it arguments for the inclusion of NSAs in IR theory that many claim are impossible to ignore. This is not to say this inclusion has not been embroiled in controversy. Indeed, many academics have pushed back against the relevancy of NSAs and questioned just how important they really are in IR theory crafting. So, it is arguable that conceptualizations of NSAs have faced stagnation, not only in their general acceptance by the IR community but also through a lack of expansion and development of its definitions.

4.1.2 The Pushback Against NSA's

As NSAs experienced a rise to prominence, many began to question how justified assertions of their importance were, especially concerning whether states were seeing declines in power and relevance. Halliday, writing on the romanticization of NSAs, is perhaps one of the most scathing critics. Calling for an end to the romance, Halliday re-examined NSAs historically and analytically to caution against the championing of NSAs as the new way forward in IR analysis (Halliday, 2001). He concludes that NSAs are not as novel or 'non-state' as they may seem, that their position as harbingers of a global liberal order is contested and does not take

away from the centrality of the state, and that a degree of skepticism is required regarding just how influential NGOs and other NSAs really are (Halliday, 2003, p. 36-37).

Others have taken a similar stance. Lakhany, for example, questioned 'how important are non-state actors?', using the rising influence of MNCs and new theoretical frameworks of global governance to arrive at an answer (Lakhany, 2006). They find that, while non-state actors do have a newfound influence, it is doubtful that state power has been diffused, and as such the focus of power should remain in examinations of the state (Lakhany, 2006, p. 46). Even Josselin and Wallace consistently arrive back at the centrality of the state – be it in the dependence that NSAs have on states for funding or in their circumscribed ability to affect state authority (Josselin and Wallace, 2003, p. 259). This pushback against NSAs has not stopped them from being a part of contemporary IR discussions. Still, it would be difficult to argue that a lack of consensus regarding their importance has not impeded efforts to further expand upon their conceptualization and integration substantively. It is not surprising that definitions and classifications of which entities are worthy of inclusion as NSAs have largely stagnated, leaving potential new actors such as individuals out of the equation.

4.1.3 Stagnating Definitions

The study and definitions of NSAs in IR academia have not traveled far from traditional classifications in which IGOs and NGOs are central (Brown, 1995; Miller, 1994, as cited in Ataman, 2003). As such, much of the scholarship revolves around these larger entities and others such as MNCs and influential armed groups whose relevance has already been established. Indeed, it is difficult to find a contemporary article in which these actors are not included as a main focal point – even across different fields of International Relations. The Ashgate Research Companion to Non-State Actors – a 578-page volume consisting of multiple chapters aiming to provide an encompassing view of NSA literature, only recognizes three types of NSAs: NGOs, IGOs, and transnational corporations. (Renailda, 2016). The work of Josselin and Wallace, mentioned previously, also attempts to provide an overarching handbook to conceptions of NSAs which has since been cited 614 times. Although Josselin and Wallace use a comparatively broad definition to include commonly excluded economic actors such as criminal elements, churches or transnational political parties, their primary focus lies in NGOs and MNCs (Josselin and

Wallace, 2003, p. 4). Indeed, all the other scholars mentioned writing on the subject, and others writing on NSAs such as Cowles, utilize what Ataman calls the 'traditional classification' of NSAs in which only IGOs and NGOs (including MNCs) are considered. (Ataman, 2003, p. 43; Halliday, 2001, p. 21; Weiss and Wilkinson, 2014, p. 209; Lakhany, 2006, p.46; Weiss et al., 2013, p. 2)

This is not to say that the classification of NSAs has not expanded. There have been, for example, advancements in definitions of NSAs in the field of security studies. Studying peacekeeping, Bah includes Ad Hoc Organizations as an NSA of relevance (Bah, 2013, p. 314). Armed groups have also begun to be viewed as salient NSAs specifically regarding the introduction of private military corporations and the proliferation of armed groups in fragile state contexts (Krahmann, 2005; Davis, 2009).

While a thorough search may find more specific cases of NSA engagement with actors outside those mentioned above, singular cases would not detract from a general trend that seems to indicate a stagnating definition of NSAs within IR academia. The purpose here, in line with this thesis, is to demonstrate that this stagnation has not left room for the inclusion of individuals as NSAs. Given the newfound strength of cyber vigilantism and the agency it can grant, this is a gap in IR literature this thesis would like to see reassessed.

4.1.4 The Recognition of Individuals in Other Fields?

Scholars interested in cybersecurity and cyberwarfare have been more open to including individuals in their analysis of NSAs. Perhaps the most prominent is the work of Johan Sigholm, who wrote on cyberspace operations from the perspective of military studies (Sigholm, 2013). Sigholm is primarily interested in how NSAs in the cyber-realm may be employed by nation-states engaging in cyberwarfare, given that their objectives coincide (Sigholm, 2013, p. 1). Sigholm is one of the first to argue that individuals, using digital technology, can indeed have a felt impact on state security, particularly through attacks on critical military or civilian infrastructure and information warfare, although their relevance stems largely from how states will choose to utilize them (Sigholm, 2013, p. 8, p. 32). Other scholars have approached NSAs in cybersecurity/warfare from the lens of international law. Blank, for example, is most interested in how NSAs who engage in international cyberwarfare would be treated by

international law in questions of prosecutions and protections granted (Blank, 2013). Similarly, Bussolati delved into how expanding digital technologies have served to shrink the role of the state in international cyber law, evaluating the challenges faced by international law makers posed by the rise of NSAs, including individuals, in cyberwarfare (Bussolati, 2015).

While only tangentially related to International Relations academia, the inclusion of individuals in the analysis of the cyber realm indicates that their importance is being felt, and that there is potential for their inclusion in IR literature. Still, prior to this thesis there has yet to be substantive engagement with cyber vigilantism within IR.

4.1.5 Cyber Vigilantism outside of IR

Much of the literature around cyber vigilantism is dominated by sociological interest in how it has developed in China. Many scholars have explored the Human Flesh Search Engine on the Chinese internet, with focus on how empowered citizens were able to investigate and collectively punish corrupt officials, but also regarding the social implications of citizen-led surveillance. (Chang and Poon, 2017; Gao, 2016; Chang and Zhu, 2020; Gao and Stanyer, 2014). As cyber vigilante incidents continued to increase in visibility, scholars began to explore the ethics of cyber vigilantism. Mathias Klang explored its ethical dimensions in an article titled, "On the internet, no one can see your cape" (Klang, 2015). Others wrote of potential hazards and legal concerns respectively (Kosseff, 2016, Väljataga, 2022). Recently, attempts have been made to consolidate the different types of cyber vigilantism to offer a more encompassing picture of the phenomenon.

Perhaps most poignant and encompassing is the conceptual framework offered by Smallridge et al. in 'Understanding Cyber-Vigilantism: A Conceptual Framework' (Smallridge et al., 2016). Smallridge et al. builds off the work of other academics, including Johnston's work on defining vigilantism (Johnston, 1996), to create a criterion-based framework of vigilantism in cyberspace (Smallridge et al., 2016, p. 66).

As a separate framework, Trottier posits cyber vigilantism as a 'weaponization of visibility'. For Trottier, cyber vigilantism finds its strength by producing unwanted visibility for its targets, such as 'name and shame' campaigns or the circulation of texts, images, etc. (Trottier, 2017, p. 56).

Finally, Chang, Zhong, and Grabosky proposed that cyber vigilantism should be seen as the 'co-production of cyber security', in the sense that it allows individuals to aid states in investigative, regulatory, and compliance efforts regarding criminal action (Chang et al., 2018). These frameworks will be elaborated upon, broken down, and synthesized in the subsequent integrative literature review to arrive at this thesis' expanded framework of cyber vigilantism as 'producers of state security and insecurity', serving to better explain how cyber vigilantism has granted individuals saliency as NSAs in an IR context.

To reiterate, the purpose of this block of literature was to prove that individuals have largely been discounted in IR academia as salient NSAs. This was done by demonstrating how and why NSA literature has risen and then stagnated as a topic within IR, and how this has worked to exclude the potential introduction of entities like cyber vigilante individuals. As individuals are beginning to be discussed as NSAs in other fields, and as cyber vigilantism has found a new strength with the introduction of open-source intelligence tools, it is possible to now bridge this gap in both IR literature and literature regarding cyber vigilantism itself by showcasing its transnational impact on state security.

4.2 Block Two: Integrative Literature Review

The purpose of this integrative literature review is to arrive at an expanded framework of cyber vigilantism which better suits the inclusion of cyber vigilante individuals as salient NSAs in an international relations context. To do so, three frameworks of cyber vigilantism (Trottier 2017; Smallridge et al., 2016; Chang et al., 2018) will be examined and critiqued along the lines of a 'guiding theory' (Torraco, 2005). To reiterate, the guiding theory used in this integrative literature review is similar to what is guiding the exploration of the research question of this thesis: Due to the 'second wave' of OSINT technology, cyber vigilante individuals have a newfound ability to have a transnational impact on security.

Once critiqued, the frameworks will be synthesized to arrive at an expanded framework of cyber vigilantism as 'producers of state security and insecurity' more closely in line with the guiding theory above.

4.2.1 Cyber Vigilantism as a 'Weaponization of Visibility'

Trottier posited cyber vigilantism as a weapon of visibility in 2017 with the aim of developing a theoretical and empirically backed understanding of the subject to further research (Trottier, 2017). Having recognized cyber vigilantism as global, Trottier definitionally delineates the phenomenon using a similar approach to Smallridge below by comparing it to Johnson's definition of 'offline' vigilantism (Johnson, 1996). Using a table, Trottier compares the 6-criterion definition of vigilantism by Johnson and makes his own corrections that apply to cyber vigilantism.

Table 1 Key features of conventional and digital vigilantism

	Conventional vigilantism (Johnston 1996)	Digital vigilantism
Planning	Premeditation	Facilitated spontaneity
Private agency	Distinguished from state and corporate actors	Possible connections with state and corporate actors
Autonomous citizenship	Self-protection	Asserting new boundaries
Use of force	Embodied	Visibility as weapon
Reaction to crime/deviance	Threat of established order	Fusion of local and mediated norms
Personal and collective security	Policing localised territory	Mediated policing

(Johnson, 1996; Trottier, 2017, p. 59).

Trottier, building off his new criteria of digital (cyber) vigilantism, identifies a few key aspects of cyber vigilantism that are theoretically of interest.

First, he notes that cyber vigilantism is occurring within the context of an expanding media culture that allows for online organization and crowdsourcing, grants access to a widespread informational infrastructure, and facilitates social harm (e.g., cyberbullying) (Trottier, 2017, p. 59). Cyber vigilantes, then, are acting in an environment that allows much easier peer-to-peer communication, meaning information can be fragmented and dispersed at a fast rate (Trottier, 2017, p. 61). Additionally, this expanding media culture and social media has rendered a blurring of lines between information considered public and private (Trottier, 2017, p. 61). Second, Cyber vigilantism often arises out of situations where a state response to a crime or misconduct is deemed inadequate, and as such cyber vigilantes will collectively take offense and coordinate retaliation plurally to act in a way they feel has been missed by the state (Trotter, 2017, p. 63). While it often arises out of a critique of the state, cyber vigilantism is inherently a renegotiation of the boundaries between state and citizen when it comes to policing and judicial

efforts – in other words a form of 'self-policing' wherein cyber vigilantes are the saviors of national sovereignty and citizenship (Trottier, 2017, p. 63). On one hand, cyber vigilantes challenge state monopolies of power and policing, but they also work to reproduce that power by being allured by the idea of citizen responsibility, ultimately falling prey to expanding components of state neoliberal governmentality (Warren, 2009, as cited in Trottier, 2017; Trottier, 2017, p. 64).

Finally, Trottier finds that the most distinguishing feature of cyber vigilantism is that it is mainly carried out by making a target's personal information visible to the public eye (Trottier, 2017, p. 65). Trottier ultimately arrives at the notion that cyber vigilantism transcends traditional understandings of surveillance by not only allowing for the collection of personal data but also directly causing social consequences to stem from this collection by posting said data on social media (Trottier, 2017, p. 65). While cyber vigilantes may feel they have some sort of responsibility in watching over the actions of others (e.g., lateral surveillance), this 'weaponization of visibility' can produce both 'social change and social harm' (Trottier, 2017, p. 68).

Relation to Guiding Theory

While Trottier's 'weaponization of visibility' framework fits with the guiding theory, it slightly misses the mark in two ways. First, Trottier places specific emphasis on cyber vigilantism as the surveillance by one (or many) citizens over another citizen by going in depth into concepts of lateral surveillance (Andrejevic, 2005, as cited in Trottier, 2017), self-surveillance, and concerns over how individuals are rendered subjects to the power of others (Trottier, 2017, p. 67). While this is in one way positive, as it indicates that Trottier places a specific emphasis on how individuals are significant to cyber vigilantism, it also means that the focus on Trottier's framework is on cyber vigilante actions in which the targets are citizens or a specific group of citizens, rather than an entity such as a state. As such, the impact cyber vigilantism can have on the security of states specifically is missed – Trottier does indeed say that more research is needed into the state-citizen relationship of cyber vigilantism (Trottier, 2017, p. 65).

Second, Trottier makes little mention of a transnational element regarding cyber vigilantism. While it is granted that cyber vigilantism can have a 'glocalised' impact (Wellman,

2002, as cited in Trottier, 2017), it is only discussed briefly in the context of nationalist manifestations, such as the outing of KKK members by the Anonymous hacking organization (Trottier, 2017, p. 65). As such, not enough attention is brought to cyber vigilantism's transnational impact (as proposed by this thesis) to affect a foreign state.

4.2.2 Smallridge et al.'s Conceptual Framework of Cyber Vigilantism

While many have proposed different ways of understanding cyber vigilantism, perhaps most focused on the creation of a usable conceptual framework is the work offered by Joshua Smallridge, Philip Wagner, and Justin Crowl in 'Understanding Cyber-Vigilantism: A Conceptual Framework' (Smallridge et al., 2016). Like Trottier, Smallridge et al., build off Johnston's work on defining vigilantism (Johnston, 1996), to create a criterion-based framework of vigilantism in cyberspace revolving six core criteria (Smallridge et al., 2016, p. 66) including:

1. Premeditated planning and organization must take place.
2. Cyber vigilantism must be carried out by actors in a private capacity.
3. These private actors must not have the support of the state.
4. Cyber vigilante acts must involve harm or threats of harm.
5. Cyber vigilantism must be in response to criminal or socially deviant actions.
6. Cyber vigilantism is carried out to control crime (Smallridge et al., 2016, p. 64-66).

Smallridge et al. elaborate on a few of the criteria that they recognize may fall prey to ambiguity. Approaching their fourth criterion, Smallridge et al. find it prudent to clearly define what they mean by 'harm'. As opposed to Johnson's idea of harming involving physical violence, harm in a cyber vigilante context presents itself as the 'causation of harm or threat thereof' (Smallridge et al., 2016, p. 65). In this sense, harm can manifest itself in non-physical ways, such as DDoS attacks or the release of sensitive information. (Smallridge et al., 2016, p. 65).

Also emphasized is the importance of criterion 3, in which actors must not have the support of the state to be considered cyber vigilantes. For Smallridge et al., any cooperation with the state during cyber vigilante actions renders the act state sanctioned, thus negating it as an act of cyber vigilantism and instead as one of 'proactive citizenship' (Smallridge et al., 2016, p. 62).

Finally, Smallridge et al. make it clear that criteria 5 and 6 are vital to understanding cyber vigilantism and separating it from actions such as cyberbullying and cyber harassment. Rather it should be stressed that cyber vigilantes act to reassure the security of a target group (Smallridge et al., 2016, p. 65).

In exploring their conceptualization, Smallridge et al. work through several cases in which strategies they deem to be cyber vigilantism are utilized. They prioritize scambaiting, hacktivism and crowdsourced cyber vigilantism (Smallridge et al., 2016) in their analysis. Ultimately, they end with a variety of opportunities for further research and would like to see their conceptual framework tested for its applicability to cyber vigilante actions (Smallridge et al., 2016, p. 67).

Relation to Guiding Theory

From the perspective of the guiding theory, Smallridge et al.'s conceptual framework requires a few changes. First, the initial criterion of premeditation and planning is largely unnecessary. While it was included in Johnson's (1996) original conceptualization of vigilantism to rule out instances of self-defense (Smallridge et al., 2016), it serves less purpose in the digital realm. Further, if considering that cyber vigilantism can occur quickly in response to an action online (such as will be demonstrated in the first case in the subsequent congruence analysis), the ambiguity around how much premeditation or planning is necessary only serves to overcomplicate the framework.

Criterion 6 also does very little in service of this thesis' guiding theory. While cyber vigilantism can be said to be in response to criminal or socially deviant actions, to say that all cyber vigilantism acts to control crime is far too zero-sum. As will be shortly demonstrated, cyber vigilantism can occur and render state's insecure even if no crimes have technically been committed. Further, as will be explored in the following synthesis of these frameworks, there is some clash with Chang et al. regarding whether states can or cannot be involved in cyber vigilantism.

4.2.3 Citizen Co-Production of Cyber Security

Chang, Zhong, and Grabosky approach cybersecurity with the notion that state resources and capabilities in policing cyberspace are largely constrained, calling for the inclusion of supplementary policing sources (Chang et al., 2018). As such, non-state actors, including individuals, have stepped in to compensate for state functions of social control that are not operating up to their standard (Chang et al., 2018, p. 102). As private actors come across illegal activity, they may feel inspired to 'fill the vacuum' caused by a lack of state capacity, and in response will engage in activities that work to help with the 'co-production of cybersecurity' (Chang et al., 2018).

Motivations for these actions of co-production differ. While some may be motivated by curiosity and self-interest, others may simply wish to protect the wider public good (Chang et al., 2018, p. 102). These differences in motivation can lead to some cyber vigilantes working outside of the law, lending to Chang et al. conceptually differing between 'unilateral co-production activities', and co-production in which states may be sponsors or coordinators (Chang et al., 2018, p. 103). In showcasing this conceptual difference, Chang et al. work through numerous ways in which the co-production of cybersecurity can be arrived at. A few stand out as notable.

First, Chang et al. indicate two types of co-production that utilize cyber vigilantism in a similar fashion to Trottier (2017) and Smallridge et al. (2016): The identification and investigation of 'illegality' in public spaces either actively searched for or happened across by chance (Chang et al., 2018, p. 103), and covert investigations by private actors of both passive (data collection) and active ('name and shame' campaigns) nature (Chang et al., 2018, p. 103; p. 105). In these instances, cyber vigilantes hold a high degree of efficacy (Chang et al., 2018).

Second, the co-production of cybersecurity can occur through immediate cooperation with the state. For Chang et al., this can either come in the form of an invitation by the state to engage in hacking or cyber vigilante activities, through existing non-state organizations that exist to help securitize cyberspace (such as the Australian Cybercrime Online Reporting Network (ACORN) providing a hotline to report illegal cyber activities), or through a mandated government requirement (such as ISP's who are required to report security breaches to their respective government) (Chang et al., 2018, p 104-105).

The second half of their work deals largely with the negative repercussions of co-produced cybersecurity – highlighting the possibility of error, collateral damage, loss of legitimacy, lack of accountability (specifically for cyber vigilantes), loss of privacy, and potential interference with policing efforts – before delving into principles they believe should be adhered to when engaging in co-production (Chang et al., 2018, p. 108-110). They recognize that co-production of cybersecurity may be a necessary pursuit for states, especially in instances of cyberwarfare where a state may need to enlist individuals with special skills in cybersecurity (Brenner and Clarke, 2010, 2011, as cited in Chang et al., 2018, p. 110). However, they warn it is a pursuit that must be done with great caution; state mechanisms should be in place to facilitate cooperation with cyber vigilantes and ensure they remain within the bounds of the law (Chang et al., 2018, p. 111). Otherwise, it is a tool that is easily abused.

Relation to Guiding Theory

The framework of co-production developed by Chang et al. is the most suited out of the three to address the transnational impact cyber vigilantism now holds. Still, it is slightly flawed in two ways. First, the focus of this framework sits squarely with how cyber vigilante individuals shape state security, but no attention is given to their equally important ability to render states insecure. For example, when discussing how states may work in tangent with cyber vigilantes, Chang et al. use the example of 'patriot hacker's' used by Russia against Estonia and Ukraine (Chang et al., 2018, p. 104). These patriot hackers are not framed as being detrimental to Estonian and Ukrainian security, but instead as bolstering Russian security by granting an element of deniability.

Second, the framework relies heavily on 'co-production' in that security in the cyber realm is achieved when state and non-state actors work together in tangent to respond to illegal acts online. As Chang et al. are largely exploring whether a degree of individual participation in cybersecurity can be useful, reference to their involvement as co-production is justifiable. However, if applied to instances of transnational cyber vigilantism, this acts to remove agency from cyber vigilantes that can otherwise have a felt impact on security without assistance from a state. While cyber vigilantes can indeed work with a state to relegate them as co-producers, this does not adequately represent their saliency. This will be further demonstrated in the cases used in the congruence analysis.

4.2.4 Synthesis: Towards 'Producers of State Security and Insecurity'.

As discussed, new tools available to cyber vigilantes through the rise of OSINT, have granted cyber vigilantes more agency than ever before. This change in the capabilities of cyber vigilantism calls for a recognition that cyber vigilantes, even when working as individuals, can have a transnational effect on state security. This ability must be included in how cyber vigilantism is theoretically approached so that cyber vigilante individuals can be properly addressed as salient NSAs.

The three frameworks explored above have all been instrumental in furthering the research and understanding of cyber vigilantism in their respective fields of criminology and sociology. As such, this synthesis is less about fully reconceptualizing their frameworks due to mistake or error and more about offering a slightly expanded framework that better encapsulates a transnational element. Indeed, even theories that are merely tweaked and applied from an existing theory can have merit in allowing for more cases to be identified and pursued for further research (Blagden, 2016, p 210.) It is hoped that cyber vigilante individuals may be more easily incorporated into discussions of NSAs in an international relations context as well. Therefore, this thesis' synthesized framework will utilize a similar use of criteria, although with a few omissions, replacements, and two key expansions.

Before arriving at a synthesized set of criteria, a clash between two theories above must be resolved. First, as has been hinted previously, there is disagreement between Smallridge et al. (2016) and Chang et al. (2018) regarding whether state sponsored actions can be considered as cyber vigilantism. For the purposes of this thesis, cyber vigilantes can indeed work with states, or under state sanctioned conditions, in line with the work of Chang et al. (2018). The rationale for this decision derives from the aforementioned 'IT Army of Ukraine'. - created when a Ukrainian senior defense minister put out a public call for cyber vigilante hackers to aid Ukraine against the Russian invasion (Tidy, 2023).

As a proposed expanded and synthesized theoretical framework, this thesis proposes to view cyber vigilante individuals as '*producers of state security and insecurity*', using the following criteria:

1. Cyber Vigilantism is carried out by private actors but can be done with assistance/sponsorship by a state.
2. Cyber vigilantes as producers of state security and insecurity primarily employ the threat of harm in their action, and this harm is generally derived from the ability to make certain information visible (e.g., as a 'weapon of visibility') to the broader global community.
3. Cyber vigilante individuals can render states secure or insecure as producers of state security and insecurity depending on motivations. This stems largely from the new OSINT tools at their disposal.
4. Cyber vigilante individuals can act at a transnational level, meaning their actions can be targeted at foreign citizens or state entities.

So, other than the omission of the two problematic criteria in the conceptual framework of Smallridge et al., there has been an attempt to implement elements from all three frameworks. Two key expansions were included in criteria 3 and 4 that recognize the agency of cyber vigilante individuals in meaningfully affecting state security transnationally. If cyber vigilante individuals are to be included as salient NSAs in IR academia, this framework can serve as a starting point for understanding how they have a globally felt impact. Next, the relevancy of this expanded framework will be tested against its predecessors through a congruence analysis across two case studies.

5. Congruence Analysis

In this section, congruence analysis will test the proposed expanded theory of cyber vigilantism as 'producers of state security and insecurity' against its three counterparts found in the previous integrative literature review. The congruence analysis will take a 'competing theory approach', following guidelines proposed by Blatter and Haverland (Blatter and Haverland, 2012, p. 163-164, as cited in Wauters and Beach, 2018). The three total theories and their hypotheses will be compared against two real-world instances of cyber vigilante action by individuals in which a state was affected. Then, the accuracy of their expected outcomes will be

weighed against each other to determine a 'best fit' theory for the cases included.

5.1. Expected Outcomes of Tested Theories

Before examining these case studies, it is essential to hypothesize the expected outcomes of each theory tested to see how well their outcomes match with what transpires in the real-world. The following expected outcomes have been pulled from the main points of the frameworks outlined in the previous section of integrative literature review serving as hypotheses.

Trottier's 'Weaponization of Visibility' Framework

In finding the expected outcomes of the cyber vigilantism framework proposed by Trottier, this thesis pulls from the main points previously explored.

1. Cyber vigilantism requires participants to be collectively offended and act in coordinated retaliation against a target. This indicates that cyber vigilante incidents should involve a plurality of participants working in cooperation.
2. Cyber vigilantism is primarily seen as instances of 'lateral surveillance' in which citizens feel they have the responsibility to police and investigate the actions of other citizens. This often comes from a sentiment of inadequacies in state capability.
3. Cyber Vigilantism finds its strength as a 'weapon of visibility' in which private data is collected and released to the public – it is in the resulting social consequences of this release that targets are made most vulnerable.

Smallridge et al.'s Conceptual Framework of Cyber Vigilantism

The conceptual framework proposed by Smallridge is perhaps most straightforward in identifying its general expected outcomes, given it is broken down into six criteria. For ease of understanding, the outcomes proposed will follow a similar format.

1. Premeditated Planning must take place, meaning action should not be spontaneous.
2. Cyber Vigilantes must be Private Actors working in a private capacity.

3. Cyber Vigilantes must not be supported by the State.
4. Harm (or the threat of harm) must be included within a cyber vigilante act.
5. Cyber Vigilantes should be intrinsically motivated to correct criminal or socially deviant behaviour and must be done in response to criminal action.
6. Cyber Vigilantism is carried out to reduce or control the effects of crime. (Smallridge et al., 2016).

Citizen Co-Production of Cybersecurity

As co-producers of cybersecurity, cyber vigilantes act to help the state to investigate, regulate, and enforce compliance to strengthen crime-stopping activity (Chang et al., 2018). The following outcomes in real-world cases should be expected:

1. Cyber vigilantism should be motivated by a desire to fill gaps left by lack of state capacity in policing actions that occur on the internet.
2. Depending on their motivations, cyber vigilantes can work directly with states to help 'co-produce security.'
3. Cyber vigilantism, regardless of its outcome, is done in an effort to increase state security.
4. Cyber vigilantism should be conducted in response to perceived criminal actions (Chang et al., 2018).

Cyber Vigilantes as Producers of State Security and Insecurity

As producers of state security and insecurity, cyber vigilantes act independently to either build upon state security or threaten to make a state more insecure, both domestically and transnationally.

1. Cyber vigilantes should have enough capacity to be able to render states more, or less secure as individuals without outside assistance. However, they can cooperate with entities such as a state if their motivations align.
2. Cyber Vigilante efforts can have a transnational reach due to the OSINT technologies available to them.
3. Cyber Vigilantism should be able to both assist in state security (e.g., as a crime-stopping tool) or to threaten state security (e.g., the geolocating of secret, critical

infrastructure). The direction taken depends on the motivation of the cyber vigilante.

Now, with the following expected outcomes from each theory outlined, two real-world instances of cyber vigilantism will be utilized to evaluate the strength of each theory and arrive at a 'best fit'.

5.2 Case 1: Geolocating the 'Disco-Ball'

(KNCA/EPA, 2016)

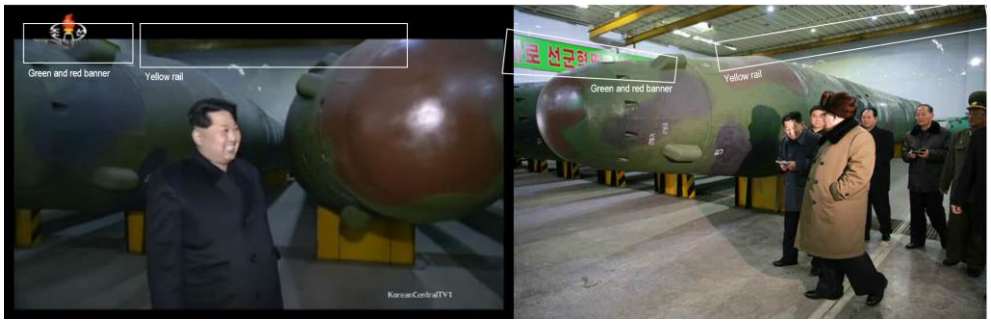
On March 9th, 2016, North Korea's propaganda arm, the Korean Central News Agency (KNCA), released this photo of Kim Jun Un surrounded by high-ranking officials, scientists, and technicians (Brumfiel, 2016). While many dubbed it the 'disco-ball' due to its peculiar shape, Kim Jun Un is actually standing in front of a nuclear warhead small enough to be placed on top of an intercontinental ballistic missile (Brumfiel, 2016).

Given the irregularity and sparsity of available media released from North Korea, many began to scrutinize the image for any useful information. One such individual was Dr. Jeffrey Lewis, a leading voice in nuclear proliferation. Lewis was able to confirm to a relatively high degree that the location of the photo was the "Thaesong (T'aeso'ng) Machine Plant outside of Pyongyang, aka the Chamjin Missile Factory (38.957764°, 125.571794°)."(Lewis, 2016).

Lewis arrived at this conclusion through a few different ways. First, he compared previously released photos of the Thaesong Machine Plant with the infamous 'disco-ball' photograph, identifying similarities in clothing, the camouflage of missiles in the background,

and banners and beams visible in both previous photographs and that of the ‘disco ball’ (Lewis, 2016).

([photographs of Kim Jun Un at separate dates at suspected missile plant], Lewis, 2016)



([photographs of Kim Jun Un at separate dates at suspected missile plant], Lewis, 2016)

Lewis then looked at the structural qualities of the building in which the missiles and ‘disco-ball’ were housed. Using an indoor shot of Kim Jun Un confirmed to be at the Thaesong Missile plant, where unique semi-circle type roofing is shown, Lewis was able to geolocate the plant as well as the extension in which the actual photo of the ‘disco-ball’ was taken through open-source satellite imagery.

([photograph of Kim Jun Un at suspected missile plant], Lewis, 2016)

([satellite imagery of geo-located missile plant], Lewis, 2016)

These findings alone are significant – a single person, using media released by the KNCA themselves and openly available tools found on the internet, was able to determine the location of a developing North Korean nuclear missile system. But this is not the end of the tale. When North Korea released photos of their nuclear warhead tests and prototypes the subsequent year, the photos were taken in a completely white and sterile room in which no identifiable markers could be determined (Zegart, 2023, as interviewed in Kurtz-Phelan, 2023).

(KNCA/EPA, 2017)

It is not certain that the choice of room for this 2017 nuclear display came as a direct result of the findings by Lewis in the previous year. Regardless, the compromising of the location of the 'disco-ball' is strong evidence that a state can have its security threatened by the work of someone across the globe on the internet.

5.2.1 Testing expected outcomes against Case 1

Trottier's 'Weaponization of Visibility' Framework

Trottier's framework seems to struggle in transnational cyber vigilante incidents, especially when conducted by an individual. While many experts did attempt to analyze the photo of the 'disco-ball', Lewis was primarily acting on his own accord. This makes it difficult to claim that this instance of cyber vigilantism arose from collective offense and a coordinated response (and would also serve to take agency away from Lewis as a cyber vigilante). Furthermore, as the target of Lewis' work is largely the North Korean state, the expected outcome of citizen-to-citizen 'lateral surveillance' does not adequately include the possibility of the North Korean state as a target. However, Lewis did release his findings to the public, and if North Korea did indeed change the location of its nuclear showcase the following year because of Lewis, this would fit well with cyber vigilantism being a 'weapon of visibility'.

Smallridge et al.'s Conceptual Framework of Cyber Vigilantism

Smallridge et al.'s criteria do fit with the actual outcomes of the case. Lewis was indeed working as a private actor without the assistance of the state that planned and organized his findings. His findings did also include the threat of harm to the North Korean state, given that his work was made entirely public. However, criterions five and six in which cyber vigilantism must be done in response to and to control crime align less. While North Korean nuclear testing is no doubt a threat to global order, it would be difficult to label the showcasing of a nuclear weapon alone as a criminal act.

Citizen Co-production of cybersecurity

As an example of cyber vigilantism where an individual renders a foreign state insecure, Chang's co-production of a security framework misses most marks. For one, it is unclear whether Lewis is more interested in threatening the security of the North Korean state rather than aiding in the securitizing of his own. It could be argued that this cyber vigilante action worked more as an insecuritizing action against North Korea than a securitizing one for his home country. Whether his motivations come from a lack of inaction by his home state (or the global community) is also unclear. Furthermore, like the shortcomings seen with Smallridge et al, Lewis is not necessarily responding to criminal action.

Producers of State Security and Insecurity

As an expanded framework, this does seem to provide the best tool in understanding how an individual can render a foreign state insecure. All three expected outcomes match well – Lewis acted on his own accord, operated on a case that is occurring outside his own borders using OSINT technology, and effectively threatened the security of the North Korean regime.

5.3 Case Two: The Fire in Natanz

In the middle of the night on July 2nd, 2020, a fire broke out near the Iranian city of Natanz, burning so bright that a weather satellite could pick out the blaze from space (Zegart, 2022). The Iranian Atomic Energy Organization (IAEO), aware of the visibility of the fire, released this photo of the aftermath of the blaze, along with a statement that a small incident had occurred with an industrial shed currently under construction (Zegart, 2022).

([photo released by the Atomic Energy Organization of Iran, of an “industrial shed” damaged by fire], AP, 2020)

As laid out by Dr. Amy Zergart, two Non-proliferation experts working as researchers at two separate NGO’s, David Albright and Fabian Hinz, were not entirely convinced by this statement (Zegart, 2022). Using geolocation technology, both acted separately to find the location of the fire, which took place not at an unassuming ‘industrial shed’ but instead at a nuclear centrifuge assembly plant at one of Iran’s main nuclear facilities (Zegart, 2022). Then, using commercial satellite imagery to get a different angle on the fire, the two experts arrived at the same conclusion – that the fire was much larger than previously reported, most likely the result of an explosion, and was possibly an act of sabotage (Zegart, 2023, as interviewed in Kurtz-Phelan, 2023). By the morning of July 2nd, Albright and Hinz took to twitter to release their findings to the internet and by the same afternoon the story had been picked up by the Associated Press and The New York Times (Gambrell, 2020; Sanger et al., 2020). By that evening, Israeli Prime Minister Benjamin Netanyahu was asked in a press conference whether Israel had been responsible for the fire in an act of sabotage as evidence and allegations piled up on the internet (Zegart, 2022).

Within one day, two non-proliferation experts, not working together, were able to gather intelligence allowing them to identify the true location of the fire, counter the claims made by Iran in a seeming cover-up, and force Israel to respond to questions about its role in the event. (Zegart, 2022). Both Iran and Israel have since refused to comment on the topic.

5.3.1 Testing expected outcomes against Case 2

Trottier's 'Weaponization of Visibility' Framework

Similar to the previous case, Trottier's framework fails to address the individual role of Albright and Hinz. The investigation into the Natanz fire was not necessarily done out of collective offense or coordinated response, but instead because of individual curiosity and doubt. The expected outcome of citizen-to-citizen 'lateral surveillance' is also not seen in this case given that Albright and Hinz were responding with skepticism towards an Iranian government agency rather than the actions of any individual citizen. The expected outcome regarding cyber vigilantism's use as a weapon of visibility is more evident. Given that Israel was implicated in the situation through the widespread publicity of Albright and Hinz after being shared on twitter, much of the social consequences and interest in the case came through their findings being made public.

Smallridge et al.'s Conceptual Framework of Cyber Vigilantism

The expected outcomes of this framework also match similarly to the first case of the North Korean 'disco-ball'. As Albright and Hinz were working as private actors, without the support of the state, with premeditation, and countered claims by Iran while forcing a public Israeli response, criteria 1-4 can be said to be adequately fulfilled. However, this framework again runs into issues with criterion 5 and 6, as Albright and Hinz are not necessarily responding to a criminal or socially deviant action (nor are they working to reduce crime), but instead are simply investigating an unordinary event.

Citizen Co-Production of Cybersecurity

The expected outcomes of the framework from Chang et al. also seem to mismatch. It is not clear that Albright and Hinz engaged in cyber vigilantism to fill a gap in state capacity, especially given the investigative and transnational nature of the case. Furthermore, their actions inherently insecuritized Iran and Israel as opposed to securitizing their home state or the general

global community – especially given that their investigation revealed an Iranian cover-up and implicated Israel as a saboteur. Finally, like the framework of Smallridge et al., the motivation for investigation into the Natanz fire came not from perceived criminal action, as is outlined in the final expected outcome of this framework, but instead from individual doubt and curiosity.

Producers of State Security and Insecurity

As another transnational case, this expanded and synthesized framework has its expected outcomes met. Albright and Hinz worked as individuals (they did not cooperate), investigated a transnational incident using OSINT tools such as geolocation and commercial satellite imagery, and possibly threatened the security of both the Iranian and Israeli state by making their findings public. As such, there is no expected outcome in conflict with this final case.

5.4 Towards a 'best fit' Theoretical Framework

As proposed by Wauters and Beach, one of the best ways for assessing the relative strength of the theoretical frameworks explored through congruence analysis is by employing the 'smoking gun' test (Wauters and Beach, 2018, p. 24). A 'smoking gun' generally refers to a piece of evidence that is conclusive as proof of a theory existing. For its use as a tool in congruence analysis and process tracing, it can be seen as: "the existence of a condition for which the cause or outcome is *necessary* amounts to evidence that is *sufficient* for the validity of a hypothesis proposing that the cause or outcome exists (Mahoney, 2012, p. 577). While some of the hypotheses and following expected outcomes may overlap, and thus cannot be used to differentiate the relative strength of the theories, those that are not overlapping can be put through a smoking gun test for theoretical uniqueness and confirmative power (Wauters and Beach, 2018, p. 24). And while smoking gun tests do not necessarily prove one theory's superiority over another, failure of smoking gun tests can be said to prove there is less supportive evidence for a theory (Wauters and Beach, 2018, p. 24).

From the cases explored above, three smoking gun tests can be identified.

1. Cyber Vigilantism can be effective even when undertaken by individuals, as both cases illustrate instances of individual action.

2. Cyber Vigilantism can be undertaken transnationally, as both cases are instances of cyber vigilantism across borders.
3. Cyber Vigilantism can affect (or at the very least target) the security of states both positively and negatively, as both instances demonstrate how state may be the made the target of individual cyber vigilante efforts.

Regarding the first smoking gun test, Trottier's framework of cyber vigilantism as a 'weaponization of visibility' is the first to fall. Given that Trottier emphasizes the collective and cooperative nature of cyber vigilantism, a lack of consideration is put into the agency of individual cyber vigilantes. As both cases showcase individual cyber vigilante efforts, Trottier's framework is not suited as a strong explanatory framework. And, as all other frameworks do not explicitly exclude individuals, they can be said to pass.

Moving to the second smoking gun test, the framework put forth by Smallridge et al. struggles. While the framework does not necessarily state that cyber vigilantism cannot occur transnationally, its sixth criterion requiring a response to criminal action does not fit well within a transnational instance. As demonstrated in the second case, cyber vigilantes acting transnationally may not be motivated to reduce crime but instead investigate an unordinary case out of curiosity and doubt. Furthermore, requiring a response to criminal action fits less well in an international context, as definitions of crime vary across states. And, while not covered by these cases, it is possible that transnational cyber vigilante action could be criminally motivated. More research into these types of cases and the ramifications of international law would be needed to fully evaluate whether this framework fully fails this smoking gun test. At this time, it can be said that the explanatory weight of this theoretical framework is reduced relative to the remaining frameworks which do not face similar issues regarding the inclusion of a transnational element.

Finally, the last smoking gun test proves to be a similar struggle for the framework proposed by Chang et al. As the focus is on how the use of cyber vigilantism allows for the 'co-production' of security, little attention is given to instances where the security of states is negatively affected. Both cases highlight cyber vigilantism that can be said to threaten, or at the very least target the security of foreign states. In these instances, it would be difficult to argue that Lewis, Albright, and Hinz were all primarily motivated to increase the security of their home

state or international community, as would be expected by Chang et al. It is equally probable that their motivations came from different sources, including from a desire to render their target state insecure. While this framework does not necessarily fail the smoking gun test, it does not sufficiently pass either. This too, reduces its explanatory weight as the 'best fit' theoretical framework for the cases included. As the expanded theoretical framework of cyber vigilantism as 'producers of state security and insecurity' allows room for state insecurity as an outcome, it is the only theoretical framework to decisively pass all three smoking gun tests.

Therefore, the expanded and synthesized framework proposed by this thesis can be said to be the 'best fit' as an explanatory framework for the cases explored. It must be recognized that, as a product of synthesis between the three other frameworks included, it is not surprising that it is able to better negotiate the smoking gun tests above. Indeed, the purpose of the framework was to encapsulate the explanatory power of its predecessors while expanding to incorporate the newfound transnational power of cyber vigilantism that has been argued for and demonstrated throughout this thesis. The goal of this framework is not necessarily to be the strongest, or even most precise, explanation of cyber vigilantism. Instead, the aim is to demonstrate that current frameworks miss certain elements of cyber vigilantism that may otherwise be of interest to IR academia. The framework of cyber vigilantism as 'producers of state security and insecurity', then, acts as the building block or springboard for the study of individual cyber vigilantes at a more rigorous conceptual level within an IR context.

6. Conclusion

This thesis sought to determine how cyber vigilante individuals could be justifiably included as non-state actors deserving of more attention within IR academia given their newfound transnational saliency. In answering this question, this thesis illustrated the 'second generation of OSINT' (Williams & Blum, 2018)., employed two blocks of literature review to first evaluate the state of the literature and then present a synthesized framework of cyber vigilantism, and tested this expanded framework using congruence analysis.

Ultimately, it has been found that there is indeed potential for incorporating cyber vigilante individuals into the field of international relations as NSAs worthy of study. Cyber vigilantism must be recognized for the impact it can have on a state-level transnationally, and scholars of IR should begin to take this impact seriously to meaningfully engage with a shifting world order. This may mean incorporating individuals, empowered by cyber vigilantism, into new conceptions of non-state actors that are justified as topics of research in their own right. This answer has been arrived at from a few findings of significance.

New technological advances have resulted in OSINT tools that have dramatically leveled the playing field between government agencies and private actors (Zegart. 2023). These tools are all powerful enough to have a transnational impact, and more importantly, target states (Zegart, 2022). When wielded by cyber vigilante individuals, they can grant both a transnational saliency and a new target in states that was otherwise not seen before their availability. The door is open for numerous social implications that demand a deeper look into the nuanced actors in our international order. This potential impact on the international community awarded by OSINT tools served as the backbone of this thesis.

It was also identified that IR literature on non-state actors has largely left individuals and cyber vigilantism out of the discussion. Despite a rise of interest in NSAs through the end of the 20th century, it is possible to explain this omission by looking at the pushback within IR academia against the importance and relevance of NSAs when compared to the state. While it cannot be proven to be corollary, this pushback contributed to a stagnation of NSA definitions in which only major players (NGOs, IGOs, and MNCs) are meaningfully engaged. Regardless, individuals have not seen much, if any, engagement by IR scholars as non-state actors. Given the previous finding above, this is a gap that this thesis believes must be addressed.

Lastly, this thesis finds that the expanded framework of cyber vigilantism as ‘producers of state security and insecurity’ holds promise as a starting point for the incorporation of cyber vigilante individuals into IR literature. Previous conceptions of cyber vigilantism have not focused on how cyber vigilantism may be relevant internationally. When compared against the two cases of cyber vigilantism seen in the congruence analysis section, the three preceding theoretical frameworks explored struggled as a match to act as a strong explanatory mechanism given the transnational nature of the cases. As the expanded framework of ‘producers of state security and insecurity’ is a synthesis of its predecessors that can better account for the reach of

cyber vigilantes across borders, it can be used as an example by IR scholars who may wish to further explore how cyber vigilantes fit into the conversations around non-state actors. Additionally, the cases used in the congruence analysis further strengthen the notion that cyber vigilantes, even when acting as individuals, hold enough saliency to effect (or at least threaten) the security of states. While surface-level examples are given in the preliminary background of this thesis, going into depth with these cases helps to further solidify the determination that cyber vigilante individuals deserve to be recognized more seriously by the field of IR.

There are, however, limitations that must be addressed. First, the purpose of the expanded framework arrived at is to act as a starting point from which cyber vigilantism can be approached through an IR perspective. As such, it was not constructed with the intention of being a fully fleshed-out and rigorously proven theoretical framework. While congruence analysis was employed through the guidelines of Bladder and Haverland, (Blatter and Haverland 2012, as cited in Wauters and Beach, 2018, p. 163-164) and employed the use of ‘smoking gun tests, further engagement with more rigorous analysis would be beneficial in its development. Its strength is as an avenue for the entrance of cyber vigilantism into IR literature; whether scholars of the field choose to develop the framework more deeply or move in a different direction requires more research.

Similarly, this thesis includes only two empirical cases of cyber vigilante individuals engaging transnationally. While congruence analysis can be sufficiently accomplished through even a single case (Wauters and Beach, 2018), it could be argued that the use of two cases is not statistically significant enough to fully defend the claims made above. The addition of more cases (such as domestic instances or securitizing instances) to this thesis’ expanded framework would help determine its theoretical power and assist in continued reconceptualization if necessary. Furthermore, research with the aim of the discovery and analysis of more empirical cases of such instances would greatly assist in positioning the transnational impact of cyber vigilante individuals past an isolated phenomena and towards a certifiable trend.

7. Bibliography

Andrejevic, M. (2005). The work of watching one another: lateral surveillance, risk, and governance. *Surveillance & Society*, 2(4), 479–497.

AP. (2021). *The photo, released by the Atomic Energy Organization of Iran, of an "industrial shed" damaged by fire in July 2020. | AP*. Opinion | Meet the Nuclear Sleuths Shaking Up U.S. Spycraft. photograph, POLITICO. Retrieved June 4, 2023, from https://www.politico.com/news/magazine/2022/01/19/nuclear-sleuths-shaking-up-us-spycraft-527319.

Ataman, M. (2003). The impact of non-State actors on world politics: a challenge to Nation-States. *Alternatives: Turkish Journal of International Relations*, *2*(1).

Bah, A. B. (2013). Civil Non-State Actors in Peacekeeping and Peacebuilding in West Africa. *Journal of International Peacekeeping, 17(3-4)*, 313-336.

BBC. (2013, April 23). *Reddit apologises for online Boston "Witch Hunt."* BBC News. https://www.bbc.com/news/technology-22263020

Blagden, D. (2016). Induction and deduction in international relations: Squaring the circle between theory and evidence. International studies review, 18(2), 195-213.

Blank, L. R. (2013). International law and cyber threats from non-state actors. In *Israel Yearbook on Human Rights*, Volume 43 (2013) (pp. 111-139). Brill Nijhoff.

Blatter, J., & Haverland, M. (2012). Designing case studies: Explanatory approaches in small-N research. Springer.

Brenner SW, Clarke LL (2010) Civilians in cyber warfare: Conscripts. *Vanderbilt Journal of Transnational Law* 43, 1011–1076.

Brenner SW, Clarke LL (2011) Conscription and Cyber Conflict: Legal Issues. In: Czosseck C, Tyugu E, Wingfield T (eds) 2011 *3rd International Conference on Cyber Conflict*, pp. 1–12. IEEE, Talinn, Estonia.

Brown, S. (1995). New Forces, Old Forces, and the Future of World Politics. Post-Cold War Edition, New York: Harper Collins College Publishers

Brumfiel, G. (2016, March 21). *Why analysts aren't laughing at these silly North Korean photos*. NPR. https://www.npr.org/sections/parallels/2016/03/21/470976577/why-analysts-arent-laughing-at-these-silly-north-korean-ph

Bussolati, N. (2015). 'The Rise of Non-State Actors in Cyberwarfare'. *Cyber War: Law and Ethics for Virtual Conflicts*,(Oxford University Press, 2015) p, 102-126.

Chandler, D., & Munday, R. (2016). *cyber-vigilantism (cybervigilantism, internet vigilantism)*. Oxford Reference: A Dictionary of Social Media. https://www.oxfordreference.com/display/10.1093/acref/9780191803093.001.0001/acref-9780191803093-e-1803;jsessionid=74FA09AE41653202908DA2EA8E71B312

Chang, L. Y. C., & Poon, R. (2017). Internet Vigilantism: Attitudes and Experiences of University Students Toward Cyber Crowdsourcing in Hong Kong. *International Journal of Offender Therapy and Comparative Criminology*, *61*(16), 1912–1932. https://doi.org/10.1177/0306624X16639037

Chang, L. Y., Zhong, L. Y., & Grabosky, P. N. (2018). Citizen co-production of cyber security: Self-help, vigilantes, and cybercrime. *Regulation & Governance*, 12(1), 101-114.

Chang, L. Y. C., & Zhu, J. (2020). Taking Justice Into Their Own Hands: Predictors of Netilantism Among Cyber Citizens in Hong Kong. *Frontiers in Psychology*, *11*. https://www.frontiersin.org/articles/10.3389/fpsyg.2020.556903

Cowles, M. (2003). Non-state actors and false dichotomies: reviewing IR/IPE approaches to European integration. *Journal of European Public Policy, 10(1)*, 102-120.

Davis, D. E. (2009). Non-state armed actors, new imagined communities, and shifting patterns of sovereignty and insecurity in the modern world. Contemporary Security Policy, 30(2), 221-245.

Downey, T. (2010, March 3). China's Cyberposse. *The New York Times*. https://www.nytimes.com/2010/03/07/magazine/07Human-t.html

Favarel-Garrigues, G., Tanner, S., & Trottier, D. (2020). Introducing digital vigilantism. *Global Crime, 21*(3–4), 189–195. https://doi.org/10.1080/17440572.2020.1750789

Gambrell, J. (2020, July 2). *Analysts: Fire at Iran Nuclear Site Hit Centrifuge Facility*. AP NEWS. https://apnews.com/article/united-nations-fires-ap-top-news-tehran-ali-akbar-salehi-50c3e7f6445ae99def6bdc65fbce6c42

Gao, L. (2016). The emergence of the Human Flesh Search Engine and political protest in China: Exploring the Internet and online collective action. *Media, Culture & Society*, 38(3), 349–364. https://doi.org/10.1177/0163443715610493

Gao, L., & Stanyer, J. (2014). Hunting corrupt officials online: The human flesh search engine and the search for justice in China. *Information, Communication & Society*, 17(7), 814–829. https://doi.org/10.1080/1369118X.2013.836553

Greenberg, A. (2021, January 20). *A site published every face from Parler's capitol riot videos*. Wired. https://www.wired.com/story/faces-of-the-riot-capitol-insurrection-facial-recognition/

Halliday, F. (2001). The romance of non-state actors. In: Josselin, D., Wallace, W. (eds) *Non-state Actors in World Politics*. 21.37. Palgrave Macmillan, London.

Herold, D. (2008). Development of a Civic Society Online? Internet Vigilantism and State Control in Chinese Cyberspace. *Asia Journal of Global Studies*, *2*, 26–37.

Huang, Q. (2021). The mediated and mediatised justice-seeking: Chinese digital vigilantism from 2006 to 2018. *Internet Histories*, *5*(3–4), 304–322. https://doi.org/10.1080/24701475.2021.1919965

Johnston, L. (1996). What is vigilantism? *British Journal of Criminology*, 36(2), 220-236.

Josselin, D., Wallace, W. (2001). Non-state Actors in World Politics: a Framework. In: Josselin, D., Wallace, W. (eds) *Non-state Actors in World Politics*.1-20. Palgrave Macmillan, London. https://doi-org.ezproxy.leidenuniv.nl/10.1057/9781403900906_1.

KCNA/EPA. (2016). *An undated picture provided by the official Korean Central News Agency earlier this month shows North Korean leader Kim Jong Un talking with scientists and technicians.* NPR. photograph, NPR. Retrieved June 4, 2023, from https://www.npr.org/sections/parallels/2016/03/21/470976577/why-analysts-arent-laughing-at-these-silly-north-korean-photos.

KCNA/EPA. (2017). *Kim Jong-un inspects a device, or perhaps a model of a bomb, in front of a diagram suggesting its size may be small enough to fit into an ICBM.* The Guardian. photograph, The Guardian News and Media. Retrieved June 4, 2023, from https://www.theguardian.com/world/2017/sep/03/did-north-korea-just-test-a-hydrogen-bomb.

Keohane, R. O. and Nye, J. S. (1989). Power and Interdependence: World Politics in Transition. New York: Harper Collins Publishers, Second Edition, 1989.

Klang, M. (2015) On The Internet Nobody Can See Your Cape: The Ethics Of Online Vigilantism. Internet Research 16: The 16th Annual Meeting of the Association of Internet Researchers. Phoenix, AZ, USA: AoIR. Retrieved from http://spir.aoir.org.

Knopf, J. (2006). Doing a Literature Review. PS: *Political Science & Politics*, 39(1), 127-132. doi:10.1017/S1049096506060264

Kosseff, J. (2016). The hazards of cyber-vigilantism. Computer Law & Security Review, 32(4), 642–649. https://doi.org/10.1016/j.clsr.2016.05.008

Krahmann, E. (2005). From state to non-state actors: the emergence of security governance. New threats and new actors in international security, 3-19.

Kurtz-Phelan, D. (Host). (2023, February 9). How Technology Is Disrupting the Intelligence World: A Conversation With Amy Zegart. In *Foreign Affairs Interview*. Foreign Affairs

Lakhany, F. (2006). How Important Are Non-State Actors. *Pakistan Horizon*, *59*(3), 37-46.

Lewis, J. (2016, June 8). The clothes geolocate the man. Arms Control Wonk. https://www.armscontrolwonk.com/archive/1201459/a-tale-of-two-visits/

Loveluck, B. (2020). The many shades of digital vigilantism. A typology of online self-justice. *Global Crime*, *21*(3–4), 213–241. https://doi.org/10.1080/17440572.2019.1614444

Mahoney, J. (2012). The logic of process tracing tests in the social sciences. *Sociological Methods & Research*, *41*(4), 570-597.

Miller, L. H. (1994). Global Order: Values and Power in International Politics. Boulder, CO: Westview Press.

Nhan, J., Huey, L., & Broll, R. (2017). Digilantism: An analysis of crowdsourcing and the Boston marathon bombings. *The British journal of criminology*, *57*(2), 341-361.

Sanger, D. E., Broad, W. J., Bergman, R., & Fassihi, F. (2020, July 2). *Mysterious explosion and fire damage Iranian Nuclear Enrichment Facility*. The New York Times. https://www.nytimes.com/2020/07/02/us/politics/iran-explosion-nuclear-centrifuges.html

Sigholm, J. (2013). Non-state actors in cyberspace operations. *Journal of Military Studies*, 4(1), 1-37

Smallridge, J., Wagner, P., & Crowl, J. N. (2016). Understanding cyber-vigilantism: A conceptual framework. *Journal of Theoretical & Philosophical Criminology*, *8*(1).

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Reinalda, B. (Ed.). (2016). *The Ashgate research companion to non-state actors*. Routledge.

Tidy, J. (2023, April 14). *Meet the hacker armies on Ukraine's Cyber Front Line*. BBC News. https://www.bbc.com/news/technology-65250356

Torraco, R. J. (2005). Writing integrative literature reviews: Guidelines and examples. *Human resource development review*, 4(3), 356-367.

Trottier, D. (2017). Digital vigilantism as weaponisation of visibility. *Philosophy & Technology*, *30*, 55-72.

Väljataga, A. (2022) Cyber vigilantism in support of Ukraine: A legal analysis. NATO Cooperative Cyber Defence Centre of Excellence. 1-6.

Warren, I. (2009). Vigilantism, the Press and Signa Crimes 2006–2007. *Australian & New Zealand Critical Criminology Conference Proceedings*,275–284. Monash University.

Wauters, B. and Beach, D. (2018). Process tracing and congruence analysis to support theory-based impact evaluation. *Evaluation*, 24(3), 284-305. DOI: 10.1177/1356389018786081

Weiss, T. G., Seyle, D. C., & Coolidge, K. (2013). The rise of non-state actors in global governance: Opportunities and limitations.

Weiss, T. G., & Wilkinson, R. (2014). Rethinking global governance? Complexity, authority, power, change. *International Studies Quarterly, 58(1)*, 207-215.

Wellman, B. (2002). Little boxes, glocalization, and networked individualism. In M. Tanabe, P. van den Besselaar, & T. Ishida (Eds.), Digital cities II (pp. 11–25). Berlin: Springer.

Williams, H. J., & Blum, I. (2018). Defining second generation open source intelligence (OSINT) for the defense enterprise. Rand Corporation.

Zegart, A. (2021, September 1). *Spies Like Us: The Promise and Peril of Crowdsourced Intelligence*. Foreign Affairs. https://www.foreignaffairs.com/reviews/review-essay/2021-06-22/spies-us

Zegart, A. (2022, January 19). *Opinion: Meet the nuclear sleuths shaking up U.S. spycraft*. POLITICO. https://www.politico.com/news/magazine/2022/01/19/nuclear-sleuths-shaking-up-us-spycraft-527319

Zegart, A. (2023, January 7). *Open secrets: Ukraine and the Next Intelligence Revolution*. Foreign Affairs. https://www.foreignaffairs.com/world/open-secrets-ukraine-intelligence-revolution-amy-zegart