Review of International Studies (2020), **46**: 5, 613–631
doi:10.1017/S026021052000008X

RIS

RESEARCH ARTICLE

Lacan in the US cyber defence: Between public discourse and transgressive practice

Jeppe T. Jacobsen*

Institute for Military Technology, Royal Danish Defence College
*Corresponding author. Email: jeja@fak.dk

(Received 28 January 2019; revised 12 February 2020; accepted 17 February 2020; first published online 20 March 2020)

Abstract

Edward Snowden exposed the discrepancy between the official US defence discourse of liberal values in cyberspace and secret surveillance and cyber exploitation practices. Situated in the critical literature on security and surveillance, the article proposes that more attention needs to be paid to the constitutive role of transgressive practices for security communities. The article introduces a Lacanian strategy for studying transgression in the US cyber defence community. Through this strategy, a transgressive other – in this case, China in cyberspace – enters the fantasy of the US cyber defence community as the symptom that conceals more fundamental tensions in the US cyber defence. But the community's representation of China in cyberspace represents more than that; China is a fantasmatic object that structures and gives content to a desire for transgressing the official ideals of the US cyber defence. This is why the excessive cyber practices that China is criticised for conducting mirror the secret, disavowed transgressions of the US cyber defence. Transgressions, the article concludes through Lacan, provide the necessary (partial) enjoyment that sustains the US cyber defence community as a solidarity-in-guilt and the official US cyber defence discourse.

Keywords: Transgression; US Cyber Defence; Jacques Lacan; Slavoj Žižek; Surveillance; Critical Security Studies

Introduction

During the Obama administration, it became publicly known that the US entities that work to defend the nation in and through cyberspace were secretly undermining the official policies they publicly promote. The US Department of Defense (DoD) officially insisted that its operations in cyberspace were being conducted under a 'doctrine of restraint' with the goal of protecting a free, open, secure, and reliable Internet and while 'being as transparent as possible'.[1] Yet, several leaked documents, including from Edward Snowden, tell a different story. These leaks revealed that the US National Security Agency (NSA) through secret programmes such as PRISM, Upstream, and Boundless Informant excessively collected data about both foreign and national citizens. For example, then NSA Director, General Keith Alexander, was quoted as promoting a strategy of 'collect it all' inside the closed walls at Fort Meade, while lying about the Agency's capacity to do so in public.[2] On the military side, anonymous sources also revealed a

[1]Ashton B. Carter, 'Remarks by Secretary Carter to US cyber command workforce at Fort Meade, Maryland', *DoD News* (13 March 2015), available at: {http://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=5602} accessed 20 November 2018; Department of Defense, 'The DoD Cyber Strategy' (Washington, DC: US Government Publishing Office, 2015), pp. 1–3.

[2]Glenn Greenwald and Ewan MacAskill, 'Boundless Informant: The NSA's secret tool to track global surveillance data', *The Guardian* (11 June 2013), available at: {https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining} accessed 20 November 2018.

© British International Studies Association 2020.

https://doi.org/10.1017/S026021052000008X Published online by Cambridge University Press

lack of restraint in NSA's secret, preparatory steps to target civilian systems in a future military confrontation with Iran.[3]

The Snowden revelations and the subsequent steady stream of leaks about secret NSA practices that transgress the norms and ideals officially promoted were the cause of widespread public outrage and debate. Naturally, academia also weighed in on the issue of secret mass surveillance, particularly within critical and sociological studies on security and surveillance. Here, most scholars situated the revelations about NSA's surveillance regime in discussions on the legitimacy of authorities' claim to act in the name of national security as well as in a broader discussion on the political power associated with the geographical, material, and discursive configurations of cyberspace.[4] What remains under-examined in the critical security studies contributions on mass surveillance post-Snowden, however, is the constitutive role of secret, excessive practices for the US cyber defence and intelligence community. This is curious. For more than a decade, one of the hallmark aims for critical security scholars has been to show how linguistic representations and everyday bureaucratic practices and technologies reproduce national or institutional identities and insecurities.[5] The article seeks to fill in the gap by examining how the constitution of the US cyber defence community[6] and the articulation of one of the main threat objects to national security, China, is interlinked through the notion of transgressive practices.

In doing so, the article turns to the growing body of literature on Lacanian and Žižekian psychoanalysis in security studies and International Relations (IR) as this branch of scholarship pays particular attention to the role of transgression in reproducing (in)security discourses.[7] The claim that arises from this theoretical edifice is, first, that transgressive practices, and *not* the official norms and rules of society, are what hold a community together,[8] and second, that transgressive practices can only find empirical form through the articulation of a place where such practices are fully enjoyed.[9] In Lacanian readings, the place that enjoys none of the prohibitions 'we' are subjected to becomes the fantasmatic place of the fascinating, exotic, inferior, repulsive, and ultimately, dangerous *other*.[10] As will be further unpacked in the analyses below, China becomes this fantasmatic place because it enables the US cyber defence community to keep the illusion that it is defending a 'whole' American *self*, while simultaneously giving content to the community's transgressive desire.

Through the existing IR and security studies applications of the Lacanian notions of fantasy, symptom, and enjoyment,[11] the article introduces a Lacanian strategy for the study of

[3]Alex Gibney (dir.), *Zero Days*, Documentary (Magnolia Pictures, 2016).

[4]Zygmunt Bauman et al., 'After Snowden: Rethinking the impact of surveillance', *International Political Sociology*, 8:2 (2014), pp. 121–44; David Lyon, 'The Snowden stakes: Challenges for understanding surveillance today', *Surveillance & Society*, 13:2 (2015), pp. 139–52; Valentin Gros, Marieke de Goede, and Beste İşleyen, 'The Snowden files made public: A material politics of contesting surveillance', *International Political Sociology*, 11:1 (2017, pp. 73–89; Claudia Aradau, 'Assembling (non)knowledge: Security, law, and surveillance in a digital world', *International Political Sociology*, 11:4 (2017), pp. 327–42.

[5]Lene Hansen, *Security as Practice: Discourse Analysis and the Bosnian War* (London: Routledge, 2006); Jef Huysmans, *The Politics of Insecurity: Fear, Migration and Asylum in the EU* (London: Routledge, 2006); Didier Bigo and Anastassia Tsoukala (eds), *Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes after 9/11* (London: Routledge, 2008).

[6]The article uses US cyber defence community as a collective term for those entities that work with cyber defence issues within the US Department of Defense (DoD), including the subsidiary military and intelligence branches (for example, NSA and US Cyber Command), and within the National Security Council and Office of the Director of National Intelligence (ODNI).

[7]Jakub Eberle, 'Narrative, desire, ontological security, transgression: Fantasy as a factor in international politics', *Journal of International Relations and Development*, 22:1 (2019), pp. 243–68.

[8]Slavoj Žižek, *The Metastases of Enjoyment: Six Essays on Women and Causality* (London: Verso, 1994), p. 55.

[9]Jason Glynos and Yannis Stavrakakis, 'Lacan and political subjectivity: Fantasy and enjoyment in psychoanalysis and political theory', *Subjectivity*, 24:1 (2008), pp. 256–74.

[10]Alain Grosrichard, *The Sultan's Court: European Fantasies of the East*, trans. Liz Heron (London: Verso, 1998).

[11]Ty Solomon, *The Politics of Subjectivity in American Foreign Policy Discourses* (Ann Arbor: University of Michigan Press, 2015); Moran M. Mandelbaum, 'State, nation, society: The congruency fantasy and in/security of the body-national/social',

https://doi.org/10.1017/S026021052000008X Published online by Cambridge University Press

transgression. As the role of transgression has yet to be properly explored in the Lacanian IR literature, the article introduces a dual strategy for studying transgression in the empirical field, adapted from Žižek's two-part ideology critique: 'the symptomal reading' and 'extracting the kernel of enjoyment'.[12] By reading the transgressive practices of the DoD and its subsidiary agencies through this dual strategy, the article also makes an empirical contribution to the study of excessive US security practices in cyberspace during the Obama presidency.[13] The article suggests that a transgressive China in cyberspace enters the fantasy of the US cyber defence community as that which conceals more fundamental tensions in the US defence. China, it is further argued, is also the fantasy that structures the very desire for transgressing the rules, norms, and ideals that the US cyber defence community officially embraces. Here, the enjoyment that China is said to represent provides the necessary content to guide the US cyber defence community towards its own transgressive surveillance and cyber exploitation practices.

The article consists of four sections. The first section provides an overview of the body of critical security literature that examines the contemporary surveillance regime post-Snowden. In doing so, the article identifies a gap in the current debate, particularly when it comes to studying the constitutive role of secret, excessive practices for those entities that conduct these practices. The second section introduces the key Lacanian concepts drawn upon in IR and security studies. Since the concept of transgression, except for cursory references,[14] has not until now entered into the theoretical toolbox of IR scholars, the second section proposes a strategy for studying transgression in empirical security analyses. The third and fourth sections apply this strategy. In the third section, the article engages in a symptomal reading of the US cyber defence community by analysing the discursive constructions of China and the United States in cyberspace. The fourth section draws a line from the transgressive practices, which China has been criticised for, to those exposed by Snowden and others within the US defence community, through a reading of desire and enjoyment in the US cyber defence community.

Critical security studies of surveillance and secrecy post-Snowden

Unsurprisingly, the Snowden revelations reinvigorated the scholarly attention to states' surveillance practices in critical and sociological studies on security. Most contributions written in the immediate aftermath of the revelations had clear normative undertones and expressed concern over the negative consequences of Big Data surveillance for political liberties and cohesion.[15] However, the contributions went beyond calling out the political illegitimacy of the revealed practices. Some scholars saw the revelations as a possibility for revisiting (and nuancing) the debate

Critical Studies on Security, 4:2 (2016), pp. 187–201; Andreja Zevnik, 'A return of the repressed: Symptom, fantasy and campaigns for justice for Guantánamo detainees post-2010', *The British Journal of Politics and International Relations*, 20:1 (2018), pp. 206–22; Charlotte Heath-Kelly, 'Forgetting ISIS: Enmity, drive and repetition in security discourse', *Critical Studies on Security*, 6:1 (2018), pp. 85–99; Nadya Ali and Ben Whitham, 'The unbearable anxiety of being: Ideological fantasies of British Muslims beyond the politics of security', *Security Dialogue*, 49:5 (2018), pp. 400–17.

[12]Slavoj Žižek, *The Sublime Object of Ideology* (2nd edn, London: Verso, 2008), p. 140; Ali and Whitham, 'The unbearable anxiety of being'.

[13]The article does not discuss the Trump presidency, as the relationship between the public cyber defence discourse and the transgressive practices is different from during the Obama presidency. Russia has emerged as a top threat from cyberspace, although rather ambiguously in the White House; the US Cyber Command has become more open about its aggressive behaviour in cyberspace; and we have not had the same number of leaked documents to provide us with insights into the secret workings of the US cyber defence community.

[14]Eberle, 'Narrative, desire, ontological security, transgression'.

[15]Bauman et al., 'After Snowden'; David Lyon, 'Surveillance, Snowden, and Big Data: Capacities, consequences, critique', *Big Data & Society*, 1:2 (2014), pp. 1–13; Lyon, 'The Snowden stakes'; Gloria González Fuster and Rocco Bellanova, 'Edward Snowden: The last Big Brother?', *openDemocracy* (13 May 2014), available at: {https://www.opendemocracy.net/en/can-europe-make-it/edward-snowden-last-big-brother/} accessed 5 July 2019.

https://doi.org/10.1017/S026021052000008X Published online by Cambridge University Press

on the privacy-security trade-off[16] or the role of secrecy in interstate relations.[17] Other scholars located the practices revealed by Snowden in a complex transnational, sociotechnical, networked architecture or security assemblage, noting that the excessive surveillance practices were not reducible to a powerful actor's pursuit of its national security interests.[18] Others again have used the public and legal debates over Snowden's files to show how knowledge (and non-knowledge, for example in the form of ignorance, secrecy, ambiguity, and error) are enacted in ways that have narrowed the space for political discussions on freedom and democracy.[19] Several critical scholars of security and surveillance have sought to identify ways of contesting the current surveillance practices. Jef Huysmans, for example, proposes a reinvention of a 'democratic curiosity' and Claudia Aradau and Tobias Blanke find inspiration in computer and information science to mobilise a 'challenge to the security professionals' claims to credible knowledge'.[20]

Many of these scholars have situated contemporary surveillance practices in a global sociotechnical assemblage, and in so doing align with the increasingly popular 'material turn' in international and security studies. Within this emerging body of work, objects are seen as having acquired capacities to constitute new meaning, subject positions, and spaces in interrelation with discourses.[21] The efforts by these scholars to map the components in the complex material and discursive global surveillance regime have been important. From these contributions we have come to understand how the geographies and materialities of Internet cables; the networking technologies and algorithmic practices; the changing lines between 'foreign' and 'domestic' and between 'public' and 'private' in the security architecture of the state; the guilds of transnational security professionals; the behaviour of users online; and the legal practices that restrict what becomes publicly known and discussed, comprise some of the multifaceted interactions and material-discursive dynamics that constitute and reproduce the global surveillance regime today.

However, what has been granted less attention in critical and sociological studies on surveillance is, first, the role of secret practices, which transgress publicly articulated norms, in the identity formations of those entities that are responsible for securing the nation through cyberspace, and, second, the interaction between the constitutive role of transgression and the reproduction of the threat environment. As part of the attempt by critical security and surveillance scholars to identify and analyse key components of the global surveillance regime, the identity formations of the US DoD and its subsidiary agencies deserve further scrutiny.

Although most recent attempts to capture the complex surveillance regime do not discuss transnational, national, or institutional identity formation, they have their roots in the traditional critical and sociological approaches to security – approaches, which in the 1990s and early 2000s

[16]Michael Friedewald et al. (eds), *Surveillance, Privacy and Security: Citizens' Perspectives* (London and New York: Routledge, 2017).

[17]Thierry Balzacq and Benjamin Puybareau, 'The economy of secrecy: Security, information control, and EU–US relations', *West European Politics*, 41:4 (2018), pp. 890–913; Didier Bigo, 'Shared secrecy in a digital age and a transnational world', *Intelligence and National Security*, 34:3 (2019), pp. 379–94.

[18]Bauman et al., 'After Snowden', p. 124; Michael Richardson, 'Surveillance publics after Edward Snowden', in P. David Marshall et al. (eds), *Contemporary Publics* (London: Palgrave Macmillan, 2016), pp. 163–80; Fernando N. Van der Vlist, 'Counter-mapping surveillance: A critical cartography of mass surveillance technology after Snowden', *Surveillance & Society*, 15:1 (2017), pp. 137–57.

[19]Gros, de Goede, and İşleyen, 'The Snowden files made public'; Aradau, 'Assembling (non)knowledge'.

[20]Jef Huysmans, 'Democratic curiosity in times of surveillance', *European Journal of International Security*, 1:1 (2016), pp. 73–93; Claudia Aradau and Tobias Blanke, 'The (Big) Data-security assemblage: Knowledge and critique', *Big Data & Society*, 2:2 (2015), pp. 1–12. See also Miguelángel Verde Garrido, 'Contesting a biopolitics of information and communications: The importance of truth and sousveillance after Snowden', *Surveillance & Society*, 13:2 (2015), pp. 153–67.

[21]Gros, de Goede, and İşleyen, 'The Snowden files made public', p. 75; William E. Connolly, 'The "new materialism" and the fragility of things', *Millennium: Journal of International Studies*, 41:3 (2013), pp. 399–412; Peer Schouten, 'Security as controversy: Reassembling security at Amsterdam airport', *Security Dialogue*, 45:1 (2014), pp. 23–42; Mark B. Salter (ed.), *Making Things International 1: Circuits and Motion* (Minneapolis, MN: University of Minnesota Press, 2015).

https://doi.org/10.1017/S026021052000008X Published online by Cambridge University Press

became known for their studies of the relationship between various transnational, national, or institutional identity formations and the production of insecurities.[22] Landmark studies of the Bosnian War and the War on Terror, for example, consolidated discourse analysis as a dominant approach in security studies by showing how security practices were (co-)constituted through intersubjective linguistic representations of boundaries between Self/Other.[23] Equally important, studies of how bureaucratic everyday security routines and technologies successfully produced a governmental identity in the EU as well as an insecurity framing of immigrants, laid the foundation for a practice-oriented approach to the study of security.[24]

Both approaches, however, direct their attention almost exclusively to the global or national discursive and/or material configurations that reproduce certain practices as *legitimate, normal*, or *ignored*. Hence, the tension between what is publicly articulated as legitimate and normal, and the secret security practices that transgress the public discourse, is not considered significant in and of itself, except as an illustration of a conflicting discourse or rationale, for example, within the broader surveillance assemblage. When examined through the lens of the psychoanalytic notion of transgression, however, the tension contains a promise of unexplored meanings.

The article makes a modest contribution towards bringing more attention to the tension between a public discourse and secret transgressive practices. The article draws on the psychoanalytical edifice developed by Jacques Lacan and popularised in political studies first and foremost by Slavoj Žižek. This literature contains many reflections on secret, transgressive practices. Such practices are tied to a range of other central Lacanian concepts, particularly fantasy, symptom, desire, and enjoyment, which have recently been granted increasing attention in security studies and IR.[25] The following section situates transgression within the existing Lacanian security studies and IR literature and introduces a Lacanian strategy for studying the tensions between a publicly articulated discourse and the transgressions that sustain it.

A Lacanian lens in security studies

Jacques Lacan does not offer an easily accessible theory – in fact, sometimes it feels as if Lacan went out of his way to encourage confusion and misunderstanding.[26] Thus, Lacan's vast network of concepts is best approached by zooming in on only a few conceptual relations at a time, and unpacking their meaning in the specific context in which they are sought applied and discussed. This section goes through some of the key Lacanian conceptual relations as they have been translated and discussed in contemporary IR and security studies. Building on this, it becomes possible to situate transgression in the broader network of Lacanian concepts, as well as introduce an analytical strategy for systematically studying transgression in security studies.

[22]David Campbell, *Writing Security: United States Foreign Policy and the Politics of Identity* (Minneapolis, MN: University of Minnesota Press, 1992); Barry Buzan, Ole Wæver, and Jaap de Wilde, *Security: A New Framework for Analysis* (Boulder, CO: Lynne Rienner Pub, 1998).

[23]Hansen, *Security as Practice*; Richard Jackson, *Writing the War on Terrorism: Language, Politics and Counterterrorism* (Manchester: Manchester University Press, 2005); Stuart Croft, *Culture, Crisis, and America's War on Terror* (Cambridge: Cambridge University Press, 2006).

[24]Huysmans, *The Politics of Insecurity*; Bigo and Tsoukala, *Terror, Insecurity and Liberty*.

[25]Badredine Arfi, 'Fantasy in the discourse of "social theory of international politics"', *Cooperation and Conflict*, 45:4 (2010), pp. 428–48; Solomon, *The Politics of Subjectivity in American Foreign Policy Discourses*; Mandelbaum, 'State, nation, society'; Heath-Kelly, 'Forgetting ISIS'; Ali and Whitham, 'The unbearable anxiety of being'; Eberle, 'Narrative, desire, ontological security, transgression'; Catarina Kinnvall and Ted Svensson, 'Misrecognition and the Indian state: The desire for sovereign agency', *Review of International Studies*, 44:5 (2018), pp. 902–21; Marco A. Vieira, '(Re-)imagining the "self" of ontological security: The case of Brazil's ambivalent postcolonial subjectivity', *Millennium: Journal of International Studies*, 46:2 (2018), pp. 142–64.

[26]Yannis Stavrakakis, *Lacan and the Political* (London: Routledge, 1999), pp. 4–5; Samo Tomšič and Andreja Zevnik (eds), *Jacques Lacan: Between Psychoanalysis and Politics* (London and New York: Routledge, 2016), p. 1.

https://doi.org/10.1017/S026021052000008X Published online by Cambridge University Press

Lacanian interventions in IR: A conceptual introduction

A helpful entry point into the Lacanian edifice in IR and security studies is the notion of the split or lacking subject and its relationship with Lacan's tripartite order of imaginary, symbolic, and real.[27] The Lacanian subject is based on the assumption that a constitutive lack lies at its core. The implication following from this assumption is a disjunction between the imaginary conception of a 'whole self' and the experience of the subject. The subject's experience, it is further assumed, is always mediated through the subject-position provided by a symbolic order of language. The symbolic order structures our desire but is simultaneously interrupted by an affective, non-symbolisable reminder of the fact that this order – just as the self – is not an organic whole.[28] This reminder is what Lacan calls 'the real'. In short, 'the subject is constantly split between a desire to speak from within and a wish to become integrated into the symbolic order that pre-exists it'.[29] From this, one of the key analytical objectives of the Lacanian analyst is to locate and track the subject's constant process of identification; that is, how actors – whether individuals or collectives – step into subject-positions carved out by a socio-symbolic order and, thereby, establish themselves as subjects.

Charlotte Epstein, for example, draws on this constitutive lack at the core of the split subject to challenge the idea of a state or nation having a cohesive self as well as to clarify the distinction between subject-positions and subjectivity in the discourse analytical approaches in IR.[30] More recent IR contributions from Epstein and from Catarina Kinnvall and Ted Svensson use the assumption about the split subject that always searches for (but fails to reach) a 'whole identity' to show how *misrecognition* is inherent in states' attempt to fulfil the desire for sovereignty and international recognition.[31]

Kinnvall and Svensson bring another popular Lacanian concept into play in their study of misrecognition and the Indian state, namely fantasy.[32] To avoid confronting the ontological lack of being, Lacan argues, a fantasy that gives the subject the means to sustain the illusion that wholeness is attainable must be invented.[33] Importantly, fantasy involves transforming the ontological lack into an empirical lack in the symbolic order;[34] that is, into a *lost object* 'whose recapture offers a (false) promise of completeness and wholeness'.[35] Writing explicitly to a critical security studies audience, Moran Mandelbaum argues that fantasy is in need of a (threatening) object that prevents the lost object from being reached. The existence of a threat or insecurity ensures that the fantasy – in his case – of congruency between state, nation and society, is not yet fulfilled, as a fulfilment would reveal that the idea of congruency is itself split or lacking.[36] Nadya Ali and Ben Whitham provide another example of what such an insecurity could look like in their analysis of the continuing sense of discomfort about the 'excesses' of 'the Muslim' in the UK.[37]

[27]Charlotte Epstein, 'Who speaks? Discourse, the subject and the study of identity in international politics', *European Journal of International Relations*, 17:2 (2011), pp. 327–50; Charlotte Epstein, 'Theorizing agency in Hobbes's wake: The rational actor, the self, or the speaking subject?', *International Organization*, 67:2 (2013), pp. 287–316; J. Peter Burgess, *The Ethical Subject of Security: Geopolitical Reason and the Threat against Europe* (London: Routledge, 2011), pp. 50–65.

[28]Jenny Edkins and Véronique Pin-Fat, 'The subject and the political', in Jenny Edkins, Persram Nalini, and Véronique Pin-Fat (eds), *Sovereignty and Subjectivity* (Boulder, CO: Lynne Rienner Publishers, 1999), pp. 1–18.

[29]Kinnvall and Svensson, 'Misrecognition and the Indian state', p. 907.

[30]Epstein, 'Who speaks?'.

[31]Kinnvall and Svensson, 'Misrecognition and the Indian state'; Charlotte Epstein, 'The productive force of the negative and the desire for recognition: Lessons from Hegel and Lacan', *Review of International Studies*, 44:5 (2018), pp. 805–28; Rebecca Adler-Nissen and Alexei Tsinovoi, 'International misrecognition: The politics of humour and national identity in Israel's public diplomacy', *European Journal of International Relations*, 25:1 (2019), pp. 3–29.

[32]Eberle, 'Narrative, desire, ontological security, transgression'.

[33]Žižek, *The Sublime Object of Ideology*, pp. 47–50, 138.

[34]To capture this process, Lacan introduces the notion *objet petit a*, which stands for the process through which our desire becomes attached to objects, as well as a structural position that ensures that the objects remain unattainable.

[35]Heath-Kelly, 'Forgetting ISIS', p. 88.

[36]Mandelbaum, 'State, nation, society'.

[37]Ali and Whitham, 'The unbearable anxiety of being'.

https://doi.org/10.1017/S026021052000008X Published online by Cambridge University Press

What sustains fantasy, however, is not only the symbolisation of the unattainable desire for completeness as an obstacle that prevents its realisation, that is, the Muslim who disturbs 'the British order'. The Lacanian notion fantasy is also sustained by the partial enjoyment that the subject derives from the unconscious imperative 'Enjoy!'.[38] Through the concept of partial enjoyment, we can return to the core concept that drives this article: *Transgression*. Žižek illustrates how partial enjoyment takes its form as the transgression of the official norms and prohibitions invoked in fantasy. He illustrates his point with references to the Holocaust, Abu Ghraib, lynching in the American South, and paedophilia in the Catholic Church as extreme examples of the enjoyment associated with being involved in secret, transgressive practices.[39] In Nazism, for example, the enjoyment of being part of an obscene, dirty secret of excessive torturing of victims in the concentration camps worked alongside ideas of honourable German soldiers and public protests against social injustices.[40] Paradoxically, Žižek argues, the collective dirty secret gives a community a common point of identification – what he calls a 'solidarity-in-guilt' – and hence, transgressions sustain a fantasy: 'What "holds together" a community most deeply is not so much identification with the Law that regulates the community's "normal" everyday circuit, but rather *identification with a specific form of transgression of the Law, of the Law's suspension* (in psychoanalytic terms, with a specific form of enjoyment).'[41]

Curiously, most introductions to and applications of Lacanian and Žižekian thoughts in IR do not include reflections on the role of transgression. It is only in his introduction of fantasy to the IR literature on narratives and ontological security that Jakub Eberle shows how transgressions support the 'rational argumentation' of official narratives. In his examination of the German opposition to the 2003 invasion of Iraq, he turns explicitly to the concept of transgression to highlight tabloid portrayals of the United States in terms of 'missionary fervour, gung-ho militarism and ruthless imperialism' as that which affectively supports the 'rational' arguments against the invasion.[42] While opening the door for the study of transgression in IR and security studies, Eberle does not fully unpack the radicality of the notion as outlined by Žižek above. Eberle uses transgression to give meaning to the non-politically correct representations of the United States in the German news media. Yet, while he is most probably right in claiming that tabloid media narratives arouse more desire than technocratic, 'objective' narratives, he fails to elaborate on the connection between transgression and prohibition/official norms. A fantasy contains an 'other' that enjoys what we are prohibited from enjoying, but the fantasy is sustained by a *dirty secret*, the transgressive practice. It would be a stretch to see the news media's ridicule of President Bush as a *dirty secret*, especially in a society that considers itself a liberal democracy and does not prohibit such media coverage. The rest of this section introduces a strategy for how to advance the study of transgression in security studies.

A dual strategy for the study of transgression

To sum up the above, transgression is connected to the Žižekian-Lacanian concept of fantasy in two ways. First, it emerges in the representations of an excessive other that transgresses the norms imposed upon the subject and thereby prevents the subject from fully enjoying its 'identity'. And second, fantasy is sustained by the subject's own disavowed transgressive practices. Žižek develops two interconnected discursive strategies for analysing fantasy that makes it possible to highlight the relation between these types of transgression: The symptomal reading and extracting the

[38]Slavoj Žižek, *Tarrying with the Negative: Kant, Hegel, and the Critique of Ideology* (Durham, NC: Duke University Press, 1993), p. 217; Slavoj Žižek, *The Ticklish Subject: The Absent Centre of Political Ontology* (London: Verso, 1999), pp. 248, 367.
[39]Slavoj Žižek, *Violence: Six Sideways Reflections* (New York, NY: Picador, 2008), pp. 167–77.
[40]Slavoj Žižek, *The Plague of Fantasies* (2nd edn, London: Verso, 2008), pp. 70–2.
[41]Žižek, *The Metastases of Enjoyment*, p. 55, emphasis in original.
[42]Eberle, 'Narrative, desire, ontological security, transgression', p. 259.

https://doi.org/10.1017/S026021052000008X Published online by Cambridge University Press

kernel of enjoyment.[43] Let me introduce these in turn before concluding the section with a reflection on the methodological implications of these discursive strategies.

The symptomal reading takes place in two steps. First, it takes its form as a discourse analysis that demonstrates how a system of signification is fixed through master signifiers.[44] Like post-structuralist discourse analyses, the initial symptomal reading rejects the notion that any discursive distinctions can fully fix meaning around a closed structure: '[T]he Social is always an inconsistent field structured around a constitutive impossibility', as Žižek puts it.[45] This means that the master signifier or the entity speaking on its behalf is not really a master but is – just like the Lacanian subject introduced about – lacking; that is, not a coherent 'whole'. To maintain the discourse and the status of the master signifier, a fantasy object – 'a theft of enjoyment'[46] – that prevents the master from living up to its promise of 'wholeness' must be constructed.[47] A symptomal reading then scrutinises the representation of the practices of 'the theft' *vis-à-vis* the official rules and norms introduced by the 'self' within the discourse. This first step to an extent resembles a conventional discourse analysis that sees identity formation as being structured around linking and differentiation, with the *other* becoming everything the *self* is not, but the symptomal reading goes further.

Thus, the second and most important step, which Andreja Zevnik as well as Ali and Whitham have introduced to an IR and security studies audience,[48] locates the uncomfortable 'truths' that the *other* displaces from the discourse. Displacement is supported by a condensation; that is, the process of which the *other* takes on opposing features, for example, the Jew in Nazism that is both 'dirty *and* intellectual, voluptuous *and* impotent', and therefore all the more threatening.[49] Yet, the uncomfortable 'truths' are set to return. The symptomal reading gives meaning to out-of-the-ordinary experiences and ruptures – the symptoms – as that which return to interrupt and expose the fantasy as fantasy.[50] In Zevnik's symptomal reading, for example, the 'overcoming the exception' is uncovered as the fantasy of modern politics. To her, the case of *Al-Adahi v. Obama* where the civil society that campaigned to eradicate the exceptional legal practices governing Guantánamo suddenly went silent exemplifies the return of the repressed.[51]

The 'repressed material' can serve as the gateway to the second Žižekian strategy for analysing transgression within fantasy, namely extracting the kernel of enjoyment. In such an analysis, it is about articulating the way in which a discourse implies, manipulates, and produces a prediscursive enjoyment structured through fantasy.[52] Rather than claiming to have access to what is prediscursive, extracting the kernel of enjoyment seeks to take into account the way the transgressive other enters the framework of fantasy structuring *our* transgressive enjoyment.[53] Using the transgressions ascribed to the other in the symptomal reading as the point of departure, this interpretive exercise pays particular attention to the areas in which certain behaviours appear unnecessary

[43]Žižek, *The Sublime Object of Ideology*, p. 140.

[44]Ibid.

[45]Ibid., p. 142.

[46]Žižek, *Tarrying with the Negative*, p. 203, fn. 7.

[47]Lacan's matrix for the Four Discourses, and particularly the Master Discourse, offers a useful methodological entry point into this initial step of the symptomal reading. Without expressively engaging in a symptomal reading, Arfi's discussion on Wendtian constructivism provides an excellent illustration of how the structural relations in the Master Discourse inevitably lead to the construction of a fantasy. Arfi, 'Fantasy in the discourse of "social theory of international politics"'. For another discursive reading of Lacan. See also Solomon, *The Politics of Subjectivity in American Foreign Policy Discourses*.

[48]Zevnik, 'A return of the repressed'; Ali and Whitham, 'The unbearable anxiety of being'.

[49]Žižek, *The Sublime Object of Ideology*, p. 141, emphasis in original.

[50]Jacques Lacan, *Psychosis*, ed. Jacques-Alain Miller, trans. Russell Grigg, Book III (New York, NY: W. W. Norton and Company, 1997), p. 60; Slavoj Žižek, 'Introduction: The spectre of ideology', in Slavoj Žižek (ed.), *Mapping Ideology* (London: Verso, 1994), p. 10.

[51]Zevnik, 'A return of the repressed'.

[52]Žižek, *The Sublime Object of Ideology*, p. 140.

[53]Ibid., p. 141.

https://doi.org/10.1017/S026021052000008X Published online by Cambridge University Press

and 'out-of-joint' when compared to the dominant argument that secret surveillance and cyber exploitation practices are 'necessary for national security' and 'for the good of the country'. These areas hint at the unconscious imperative 'Enjoy!' that is at play. When successful, such a reading produces the experience that there is nothing 'behind' the fantasy; that fantasy is simply a screen masking a void.[54]

The Lacanian approach to the study of discourse offers two methodological paths: A linguistic reading of discourse as communication and reading discourse as a social bond. While Žižek is a proponent of the latter, this article takes a linguistic point of departure. Similar to Ty Solomon's linguistic Lacanian reading of the US foreign policy discourses,[55] the case study in this article sets out by locating the fantasmatic representations of what is lost and who is blamed for the loss both in the official documents and speeches and in the less official texts such as statements made by those that are invested in and, thus, also reproduce the discourse. In the following study of the US cyber defence community in the Obama era, these texts include the 2015 DoD Cyber Strategy, the Office of the US Director of National Intelligence's annual worldwide threat assessments, and statements made by acting Defense Secretaries and Directors of National Intelligence. They also include interviews with and analyses by US military officers working with US cyber defence and information security.[56]

However, whereas Solomon's emphasis is on how a discourse 'grips' its subjects through its affective appeal, the reading strategy deployed in the following to extract the kernel of enjoyment pays particular attention to that which is at the outskirt of the discourse – the statements and practices that do not appear to add up but nevertheless carry meaning about the workings of the discourse. The Snowden leaks and anonymous sources that reveal what goes on behind closed doors provide important empirical data. Not only do they expose the discrepancies between public discourse and secret practice that is the focus of this article, they also provide the sources for locating the slips of the tongue within the discourse; that is, the unnecessary exaggerations or outbursts that provide insights into the kernel of enjoyment tied to the transgressive practice.[57]

To demonstrate the utility of this dual approach to fantasy and transgression in critical security and surveillance studies, the next section engages in a symptomal reading of the US cyber defence community, before the last section turns to its kernel of enjoyment.

Reading China as the symptom of the (impossible) US cyber defence

The symptomal reading of the US cyber defence community comes in two steps. First, it engages in a discursive reading of the community's self-representation as well as representations of the object that prevents the community from reaching its 'true potential'. The second step examines the displacement of 'truths'. Let me start with the first reading.

[54]Slavoj Žižek, *Iraq: The Borrowed Kettle* (London: Verso, 2004), p. 142.

[55]Solomon, *The Politics of Subjectivity in American Foreign Policy Discourses*.

[56]Supplementing the reading of official sources, the article draws here on eight interviews with US officials working with defending the US in cyberspace, two from the US Cyber Command, four from the US Military Academy, West Point, one from US Indo-Pacific Command, and one from NATO Headquarters. One conversation took place in 2015, while the others took place in late 2016 and early 2017. Two additional interviews have been made with employees at FireEye and Crowdstrike. None of the individuals were willing to be quoted with name and rank and have thus been anonymised.

[57]Paying analytical attention to the slip of the tongue could open the psychoanalytic lens to critique from more methodologically conservative voices of 'an interpretation gone too far'. Such critique somewhat misses the point. This is because the surprising interpretations are not simply attempts to offer 'objective truths' about the empirical object of investigation. Lacanian interventions are about making the subjects (in this case, in the US cyber defence community) think again, and ultimately to better reflect on (and master) the position they occupy within the US cyber defence discourse. This psychoanalytic ambition follows its own discursive structure, what Lacan called the Analyst Discourse. Jacques Lacan, *On Feminine Sexuality: The Limits of Love and Knowledge*, ed. Jacques-Alain Miller, trans. Bruce Fink, Book XX: Encore (New York, NY: W. W. Norton and Company, 1998), pp. 14–25; Jacques Lacan, *The Other Side of Psychoanalysis*, ed. Jacques-Alain Miller, trans. Russell Grigg, Book XVII (London, New York, NY: W. W. Norton and Company, 2007), pp. 11–68.

https://doi.org/10.1017/S026021052000008X Published online by Cambridge University Press

The Office of the US Director of National Intelligence (ODNI)'s annual *Worldwide Threat Assessment of the US Intelligence Community* as well as the US Department of Defense Cyber Strategy are the authoritative documents for determining what counts as threats to the United States and what national security looks like. Those in the US cyber defence community who speak through these documents speak on behalf of the master signifier: Whatever is proclaimed as threatening in these documents has the status of truth, and they give meaning and clear direction to a broader system of signification, namely national security politics in cyberspace. The documents, in short, fixate what the US cyber defence community is defending and what it is defending against.

The 2015 DoD Cyber Strategy allows, for example, a clear representation of the American *self*, which the DoD is tasked to protect in cyberspace:

> The United States is committed to an open, secure, interoperable, and reliable Internet that enables prosperity, public safety, and the free flow of commerce and ideas. These qualities of the Internet reflect core American values – of freedom of expression and privacy, creativity, opportunity, and innovation. And these qualities have allowed the Internet to provide social and economic value to billions of people.[58]

Through (Lacanian) discourse analytical lenses, the Internet emerges as that which enables the United States to be who it really is: free, creative, opportunistic, and prosperous. The United States is altruistic, a global force of good that brings social and economic well-being to billions of people. The document further links the United States, or particularly the DoD, to transparency and restraint: 'We're going to execute our mission while being as transparent as possible, because that's also who we are.'[59] And similarly, in the DoD Cyber Strategy: '[T]he United States will always conduct cyber operations under a doctrine of restraint … and in accordance with the law of armed conflict.'[60]

Officially, the US military implements these values. Pentagon's use of cyber weapons against ISIL in Syria and Iraq illustrates the attempt to be transparent and show restraint.[61] Here, the Pentagon went public and announced that it 'dropped cyberbombs' in the attempt to disrupt propaganda, command and control servers, as well as payment of fighters. Not only did this decision signal openness, it also signalled restraint: instead of exploiting the anonymous potential of cyberspace to maintain deniability, the United States showed through its actions that it follows the Laws of Armed Conflict – specifically the principles of proportionality and distinction.[62] Officials cited by the *Washington Post* emphasised, for example, that commanders could choose cyberattacks only when it reduced the odds of civilian casualties.[63]

Yet, the US threat assessments clearly indicate that US cyber defence has not been successful in defending the nation in cyberspace.[64] And as the rest of the section shows, the cyber threats from

[58]Department of Defense, 'The DoD Cyber Strategy', p. 1.

[59]Carter, 'Remarks by Secretary Carter to US cyber command workforce at Fort Meade, Maryland'.

[60]Department of Defense, 'The DoD Cyber Strategy', p. 6.

[61]David E. Sanger, 'U.S. cyberattacks target ISIS in a new line of combat', *The New York Times* (24 April 2016), available at: {https://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region&region=top-news&WT.nav=top-news&_r=0} accessed 20 November 2018.

[62]Jeppe Teglskov Jacobsen and Jens Ringsmose, 'Cyber-bombing ISIS: Why disclose what is better kept secret?', *Global Affairs*, 3:2 (2017), pp. 125–37.

[63]Ellen Nakashima and Missy Ryan, 'U.S. military has launched a new digital war against the Islamic State', *Washington Post* (15 July 2016), available at: {https://www.washingtonpost.com/world/national-security/us-militarys-digital-war-against-the-islamic-state-is-off-to-a-slow-start/2016/07/15/76a3fe82-3da3-11e6-a66f-aa6c1883b6b1_story.html} accessed 20 November 2018.

[64]William J. Lynn III, 'Defending a new domain', *Foreign Affairs*, 85:5 (2010), pp. 97–108; James Clapper, 'Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community' (Senate Armed Service Committee Hearing,

https://doi.org/10.1017/S026021052000008X Published online by Cambridge University Press

China are articulated as that which prevents the United States from being able to fully enjoy the 'core American values' it represents and promotes in cyberspace. In the Lacanian vocabulary, the US cyber defence community's representation of China echoes the subject's attempt to conceal its dividedness by inventing a fantasmatic object that prevents it from enjoying a 'whole' secure identity. In other words, 'China in cyberspace' emerges as a central fantasy figure who steals our enjoyment by transgressing the legal and normative restraints that bound the US cyber defence. Chinese transgressions of the values promoted by the United States in cyberspace give the US cyber defence an excuse for why it fails to bring security to an open, free and prosperous cyberspace.

In the US threat assessments, China appears to be among the states 'shaken by the role the Internet has played in political instability', which is why it pursues a different model for governing the Internet – a model that involves technological measures to control content in the name of political stability.[65] This model of state-centric content control threatens to undermine 'our policy goals, particularly those to protect freedom of expression and the free flow of online information and ensure a free marketplace for information technology products and services'.[66] The Chinese government's ambition of political stability – that is, the consolidation of power through prioritising economic growth and military preparedness – is also articulated as the background for the threat from excessive cyber-enabled Chinese intellectual property theft.[67] To the US defence, Chinese economic cyber espionage transgresses the rules promoted by the United States with regard to economic competition between states, and is articulated as a serious national security concern: Everything of value flows to China; it is 'the biggest transfer of wealth in history' as then Director of the NSA and commander of the US Cyber Command, General Keith Alexander famously proclaimed.[68] And 'China in cyberspace' is a threat object that takes on additional meanings, for example, when it is further articulated in less official sources.

The 'real scary part' of the Chinese content control, as a US Army Officer underlined in an interview, is not simply the filtering of content: state ownership, control of service providers, and constant technological optimisation allow the Chinese government to surveil and identify all users, and in so doing create a constant risk of punishment, which leads to self-censorship. 'This is the real power of the Chinese domestic cyber policy', the Officer stated, and further emphasised that: '[It] ends up making people want what the government wants.' Such homogenisation is not only the ultimate form for regime stability but it transgresses the core US principle of protecting the privacy of the individual as well. Homogenisation is also tied to another threat from China in cyberspace: the threat from patriotic hackers.

When a state enjoys full obedience from its citizens, it is threatening because it allows for hackers with no clear connection to the Chinese government to pursue the government interests while offering 'plausible deniability'.[69] This obfuscates the international legal distinction between state and private responsibility promoted by the United States. 'In Chinese society, independence from government direction and control does not carry with it the idea of separation from the state', as former US Army linguist Scott J. Henderson has underlined when discussing the opaque

Washington, DC, 12 March 2013); James Clapper, 'Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community' (Senate Armed Service Committee Hearing, Washington, DC, 29 January 2014); James Clapper, 'Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community' (Senate Select Intelligence Committee, Washington, DC, 9 February 2016).

[65]Clapper, 'Statement for the Record', pp. 1–3.

[66]Ibid.

[67]Clapper, 'Statement for the Record', p. 2.

[68]Cited in Josh Rogin, 'NSA chief: Cybercrime constitutes the "greatest transfer of wealth in history" – foreign policy', *Foreign Policy* (9 July 2012), available at: {https://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/} accessed 20 November 2018.

[69]Office of the National Counterintelligence Executive, 'Foreign Spies Stealing US Economic Secrets in Cyberspace', Report to Congress (Washington, DC: Office of the Director of National Intelligence Publications, October 2011).

https://doi.org/10.1017/S026021052000008X Published online by Cambridge University Press

connection between Chinese hackers and the government.[70] And because the Chinese government is believed to exert implicit power over loyal, patriotic hackers, as Colonel Jayson M. Spade suggests, it is sufficient for the Chinese government to organise 'hacking competitions to encourage hackers to develop CNE [cyber espionage] techniques and software'.[71] In other words, in the US defence articulation, there seems to be something within the Chinese subject that makes it prone to fulfilling the will of the government. While Spade also identifies concerns in the Chinese government over potential negative implications of patriotic hacking, an influential RAND report written for the Office of the Secretary of Defense on the Chinese Military concludes that the Chinese government, if worried about negative consequences, simply gives indirect orders to the patriotic hackers through 'unsigned editorials' in the state-run media.[72]

In short, the US cyber defence community represents China's behaviour in cyberspace as a threat that transgresses the values and norms the United States officially follows and promotes. China is everything the United States is not. The Chinese government has an omnipresent gaze, enabled by excessive use of surveillance techniques and censorship, which challenges and violates the respect for and protection of freedom of expression and privacy that the United States promotes online. The Great Firewall represents to the US cyber defence community an attempt to secure the power of the Chinese government and the United States seeks to secure liberal values for all in cyberspace. Thus, Chinese government's primary interest in consolidating its own centralised power by draining the economic power of others through cyber theft of intellectual property undermines the United States' official ambition of becoming the global force for good that brings economic prosperity to billions all over the world. Lastly, the opaque Chinese government/patriotic hacker relationship is a transgression of the idea of a transparent and law-abiding state that the United States publicly promotes and defends.

Let me now turn to the second step in the symptomal reading; namely highlighting what tensions in the US cyber defence the Chinese fantasy displaces, how the Chinese threat object is taking on different opposing features, and where the 'repressed' returns.

First, 'China in cyberspace' displaces the fact that there are more uncomfortable and disavowed 'truths' about the cyberspace politics in the United States, 'truths' that are pushed to the margins of the US cyber defence discourse. Prior to the Snowden revelations, this was, for example, the fact that American privacy online is under pressure, not only from Facebook but also from the intelligence agencies' attempt to prevent terrorism. Similarly, one can detect a process of displacement in relation to the fact that the United States' pursuit of military superiority in cyberspace involves exploiting vulnerabilities in IT systems used by Americans as well as allies, which ultimately reproduces an environment that is technically insecure. Pushed to the margins by the Chinese fantasy is also the fact that the US cyber defence community itself is riddled with tensions, for example, over funding or who should have authority over the US cyber capabilities – that is, whether to use software exploits (cyber weapons) for intelligence (NSA) or military (US Cyber Command) purposes. Thus, 'China in cyberspace' is a symptom of more fundamental tensions. It plays a role as the object that prevents the US cyber defence community from confronting the fact that it is neither defending cyberspace nor is a homogenous whole. In other words, China is not only our *other*, it is that which enable us to keep the illusion that we are a 'whole' American *self*, and that which allows us to identify with this *self*. It prevents the US cyber defence community from confronting the fact that the very social field it represents is structured around an impossibility – that fulfilling a fantasy does not deliver the enjoyment it promises.

[70]Scott J. Henderson, *The Dark Visitor: Inside the World of Chinese Hackers* (self-published manuscript: Lulu, 2007), p. 102. See also Timothy L. Thomas, 'China's electronic long-range reconnaissance', *Military Review* (2008).

[71]Jayson M. Spade, 'Information as Power: China's Cyber Power and America's National Security' (Carlisle Barracks, PA: US Army War College, 2012), p. 17.

[72]James C. Mulvenon et al., 'Chinese Responses to U.S. Military Transformation and Implications for the Department of Defense' (Santa Monica, CA: Rand Cooperation, 2006), p. 93.

https://doi.org/10.1017/S026021052000008X Published online by Cambridge University Press

Second, the displacement is supported by a condensation: the Chinese cyber threat takes on contradictory features. While more 'traditional' discourse analyses would see such inconsistencies as evidence of a less stable discourse,[73] the symptomal reading draws the opposite conclusion. It was noted above, how the Chinese government through its Great Firewall is perceived to exert total control over its citizens and how the government enjoys total homogenisation with these subjects. Yet, it is also commonly understood among members of the US cyber defence community that the technical restrictions deployed by Chinese government authorities are easily circumvented by Chinese netizens and that the general level of cybersecurity in China is low. This is illustrated, for example, by a US Cyber Command official who explained in an interview that the NSA with ease had penetrated networks in Chinese universities, mobile phones, fibre-optic cables and servers controlled by the Chinese government, and second, by an official US policy that invests millions of dollars in technologies to promote freedom online, including tools for citizens to circumvent censorship regimes.[74]

According to the logic of condensation, the perception of the weaknesses of Chinese cybersecurity exacerbates, rather than dampens the perception of China as a threat. In an interview, a US official working with cyber defence policy worried that the insufficient Chinese cybersecurity allows other groups to route their cyberattacks through Chinese networks, while permitting China to deny responsibility for any hostile cyber activity with reference to a possible third party having penetrated its IT infrastructure. In other words, China is both a cyber superpower and cybersecurity novice – and threatening for both reasons. However, what hold these conflicting narratives together is what they have in common. In both cases, the Chinese government enjoys what the US cyber defence community cannot have: plausible deniability due to poor cybersecurity and totalitarian control with its citizens. This is the role of condensation.

Importantly, while China is a symptom that displaces other more fundamental 'truths', these 'truths' return. Thus, the Snowden revelations symbolise 'a return of the repressed'. Snowden and other whistleblowers revealed how the US cyber defence community is not simply defending a unified United States from Chinese threats from cyberspace but is conducting excessive surveillance and cyber exploitation practices; as will be elaborated in the following, the US cyber defence entities undermine global network security, collect data on its own citizens, and bribe private companies to share more user data than necessary – and they lie to Congress about it. As I will argue, these transgressive practices should not be understood as being detached from the official US cyber defence discourse characterised by restraint, transparency and clarity, but as constitutive hereof. Transgression is closely connected to the fantasmatic distinction between an idealised harmonious *self* and the Chinese symptom. The last section elaborates this claim by extracting the kernel of enjoyment that work to sustain the US cyber defence discourse.

The symptom's transgressions are my own transgressive desire

The above suggests that 'China in cyberspace' is a fantasmatic symptom that prevents the US cyber defence from confronting the fact that the fantasy of the United States as a force of good in cyberspace is structured around a constitutive impossibility and will not ever be able to deliver what it promises. The second Žižekian reading elaborates how exactly fantasy functions to sustain the discourse and the ideals it contains. To reiterate what was introduced earlier in the article, fantasy is the staging of our desire but simultaneously also the postponement of fulfilment of desire through displacing the object of desire to a place beyond our reach. The displacement, however, does not only take place through an *other* that deprives us of our enjoyment. It also links to the very Law, the prohibitions, rules and norms, we see as our officially affirmed

[73]Hansen, *Security as Practice*, p. 26.

[74]Jon R. Lindsay, 'The impact of China on cybersecurity: Fiction and friction', *International Security*, 39:3 (2015), pp. 18–19.

https://doi.org/10.1017/S026021052000008X Published online by Cambridge University Press

ideals.[75] Prohibitions introduce a place 'beyond' – a place where full enjoyment resides. Hence, secret transgressions become a way to seek this enjoyment while sustaining the ideal.[76] Thus, the true master of the discourse is in fact *not* the master signifier, but the master imperative: Enjoy!, which unconsciously rules the discourse.[77]

I have already illustrated above how the US cyber defence ideals of restraint, transparency, and respect for liberal values constitute a set of rules and norms juxtaposed to the excessive theft, control, and opaque nature of the Chinese government. When viewed through the second Žižekian strategy, this juxtaposition is the only way through which our transgressive desire can find a publicly articulated form (as someone else's desire). Importantly, as I seek to demonstrate below, the transgressive desire is *our* desire and hence, the *other*'s excess ends up being our own. The brief, elusive (*partial*) enjoyment that the US cyber defence community achieves through these transgressions is, the following reading suggests, what holds the community together.

The three following subsections revisit the content of the 'Chinese cyber threat' introduced in the previous section (content control, homogenisation, and centralised power) but now through the lenses of the secret, disavowed transgressive desire and enjoyment of the US cyber defence community.

Secretly living out the transgressive desire for the omnipotent gaze

The Great Firewall of China is the ultimate gaze, and it is in clear juxtaposition to the liberal respect for privacy in the United States. However, as the Snowden revelations revealed, the former Director of NSA and Head of US Cyber Command General Alexander's strategy to collect data shares similarities with the narrative of Chinese surveillance. As an intelligence officer describes: 'Rather than look for a single needle in the haystack, Alexander's approach was, "Let's collect the whole haystack. Collect it all, tag it, store it."[78] NSA programmes such as Boundless Informant that do just that, show how Alexander's strategy was implemented in practice.[79]

The practices not only point to a desire that mirrors what the other has. They also reveal the transgressive nature of the US cyber defence community. Its transgressive nature is illustrated in his rejection of the programmes' existence. In a congressional hearing in March 2012, Alexander answered a question regarding the collection of data on private Americans by saying: 'No. No. We do not have the technical insights … nor do we do have the equipment in the United States to actually collect that kind of information.'[80] Similarly, the Director of National Intelligence (DNI), James Clapper, denied in an open session in the Senate's Intelligence Committee that the NSA collected any type of data on millions of American – a lie he could easily and legitimately have avoided by refusing to answer confidential questions in open session.[81] A Lacanian (Žižekian) reading sees such slips as evidence of the economy of enjoyment that is located underneath publicly articulated statements.

Such practices of the US cyber defence community can be said to be transgressive because they go beyond what is justifiable with reference to national security and what is 'for the good of the

[75]Glynos and Stavrakakis, 'Lacan and political subjectivity', p. 263.

[76]Ibid., p. 268.

[77]Žižek, *The Ticklish Subject*, pp. 248, 367; Bülent Diken and Carsten Bagge Laustsen, 'Enjoy your fight! – fight club as a symptom of the network society', *Cultural Values*, 6:4 (2002), pp. 349–67.

[78]Ellen Nakashima and Joby Warrick, 'For NSA chief, terrorist threat drives passion to "collect it all"', *Washington Post* (14 July 2013), available at: {https://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html?utm_term=.d6d4eff5d534} accessed 20 November 2018.

[79]Greenwald and MacAskill, 'Boundless Informant'.

[80]Ibid.

[81]Steve Contorno, 'James Clapper's testimony one year later', *Politifact* (11 March 2014), available at: {http://www.politifact.com/truth-o-meter/article/2014/mar/11/james-clappers-testimony-one-year-later/} accessed 20 November 2018.

https://doi.org/10.1017/S026021052000008X Published online by Cambridge University Press

country'. Although Alexander praises the 'integrity and nobility' of the NSA and its employees as well as justifies all the practices as both necessary and legal,[82] the Snowden revelations and their aftermath add another dimension to the story. Scrutinising the NSA's practices, Judge Richard Leon revealed, for example, that the Foreign Intelligence Surveillance Court had already expressed concern over an overcollection of data that was not authorised for collection.[83] And ultimately, the defence and intelligence officials failed to name 'a single instance in which analysis of the NSA's bulk metadata collection actually stopped an imminent attack, or otherwise aided the Government in achieving any objective that was time-sensitive in nature'. Thus, Judge Leon found the collection practices to be unconstitutional.[84]

Stories based on leaked documents that give outsiders a glimpse into what is at play in the NSA are not simply perceived by the defence and intelligence community as problematic because they could lead to restraints on the community, but because they threaten the very identity of community. This is why – a Lacanian analysis would propose – the animosity towards Snowden continues to be intense in the US cyber defence community despite the fact the revelations have neither fundamentally changed the authority and surveillance practices nor led to the loss of lives as Alexander predicted.[85] To use Žižek's phrase,[86] Snowden broke with the NSA's 'solidarity-in-guilt' by leaking the information, thereby revealing how the much-treasured secrecy of the intelligence community covers the transgressive practices that work to tie a community together.

Paying for love? The transgressive desire for homogenisation

As noted above, the US cyber defences' analysis of China perceives a threat in the homogeneity between the Chinese government and Chinese patriotic citizens who do what the government wants without being explicitly directed. In apparent contrast, the United States perceives itself as a nation that respects individual freedom and the separation between the public and the private sector. Of course, patriotism also plays a very important role in the US military, including the cyber defence. When federal cyber defence recruiters travel around America to train and recruit cyber talents to the NSA or the National Cyber Guard, they are vocal about the importance of promoting patriotic sentiments and emphasise the thrill of defending the country as a selling point of joining its ranks.[87] The difference, however, is that the public call for patriotic consent promoted by the US cyber defence community is a call that should be lived out *as part of* the government and not as, the perception of China in the US suggests, as individual hacktivist citizens acting autonomously towards foreign adversaries.

On closer inspection, the distinction between the Chinese patriotic hacker who does the government's implicit bidding and the strict separation between public and private in the United States becomes a false choice, however. The US cyber defence benefits from loyal private sector

[82]Christopher Joye, 'Interview transcript: Former Head of the NSA and Commander of the US Cyber Command, General Keith Alexander', *The Financial Review* (9 May 2014), available at: {http://www.afr.com/technology/web/security/interview-transcriptformer-head-of-the-nsa-and-commander-of-the-us-cyber-command-general-keith-alexander-20140507-itzhw} accessed 20 November 2018.

[83]Devlin Barrett, 'Surveillance court judge criticized NSA "overcollection" of data: Decision offers scathing assessment of agency's management of Internet-surveillance program', *The Wall Street Journal* (11 August 2014), available at: {https://www.wsj.com/articles/surveillance-court-judge-criticized-nsa-overcollection-of-data-1407806807} accessed 20 November 2018.

[84]Michael Isikoff, 'NSA program stopped no terror attacks, says White House panel member', *NBC News* (20 December 2013), available at: {https://www.nbcnews.com/news/other/nsa-program-stopped-no-terror-attacks-says-white-house-panel-f2D11783588} accessed 20 November 2018.

[85]Joye, 'Interview transcript'.

[86]Žižek, *The Metastases of Enjoyment*, p. 55.

[87]Darren Samuelsohn, 'Inside the NSA's hunt for hackers', *Politico* (9 December 2015), available at: {http://www.politico.com/agenda/story/2015/12/federal-government-cyber-security-technology-worker-recruiting-000330} accessed 20 November 2018.

https://doi.org/10.1017/S026021052000008X Published online by Cambridge University Press

entities as well. Defense Secretary Ashton Carter promoted and endorsed partnerships with the private sector cyber security companies such as CrowdStrike and FireEye.[88] And these partnerships remain for the most part unofficial and do not consist of explicitly stated responsibilities and tasks. Nevertheless, these private companies produce reports almost exclusively pointing to Russia and China as the cyber intruders, while choosing not to report on United States activities.[89] The reports attract much global attention and have in some cases even pushed the political agenda, for example by influencing the public narrative on Chinese cyber espionage that led to the US indictment of five Chinese hackers in 2014.[90] In short, one can detect a certain degree of homogenisation between the will of the US cyber defence community and the private US cyber security companies.

Yet, there is still an important difference between the US cyber defence community and their representation of China. 'Patriotic' companies such as FireEye has a roster with a high number of former military and intelligence staff. As such, they continue to reproduce the bias they embraced while in the US cyber defence when they sell their services to the US government and US companies. In contrast, the Chinese subject is perceived not simply as biased or driven by profit but as truly loyal. Chinese patriotic hacking is a 'gesture of love' to use a phrase applied by Alain Grosrichard in his Lacanian reading of the 'Oriental' subject *vis-à-vis* the despotic Sultan.[91] That is, in the American representation, the Chinese subject seems to be predisposed to support the Chinese government even before any device of force and persuasion is applied. The difference allows us to shed light on the transgressive practices for homogenisation in the US cyber defence community.

The Snowden revelations and other leaks revealed that it costs the NSA hundreds of millions of dollars to keep its surveillance programmes running. The money is paid to private companies to cover the additional costs they incur in providing the NSA with access to their communication networks and for filtering traffic flows. Importantly, as the US companies are already legally required to turn over the information, the NSA's reimbursement creates an incentive to share as much as possible with the government – and to do so proactively, even when not legally required to.[92] Secretly paying off or bribing companies without having to is not only suggestive of the fact that US tech companies do not – out of patriotic love – do what the US cyber defence wants, it also suggests that the NSA is trying to buy the love they secretly desire. Yet, by having to pay for love, the NSA must repress the fact that it still not enjoying a 'true' homogenisation.

The transgressive desire for centralised enjoyment

The last couple of examples offered in this section suggest that the priority of the NSA is not always first and foremost the protection of global values – nor even US national and commercial interests. Not infrequently, the NSA – similar to the descriptions of the Chinese Communist Party – chooses to pursue its own departmental interests at the expense of both broader US national interests and common, global cybersecurity interests. The pursuit initially appears to

[88]Cheryl Pellerin, 'Carter unveils new DoD cyber strategy in Silicon Valley', *DoD News* (23 April 2015), available at: {https://www.defense.gov/News/Article/Article/604511/} accessed 20 November 2018.

[89]Interviews with FireEye and CrowdStrike employees.

[90]Anthony H. Cordesman and Joseph Kendall, 'Chinese Strategy and Military Modernization in 2016: A Comparative Analysis', CSIS Report (Washington, DC: Center for Strategic & International Studies, 2016), pp. 157–9; Jack Goldsmith, 'Why did DOJ indict the Chinese military officers?', *Lawfare* (20 May 2014), available at: {https://www.lawfareblog.com/why-did-doj-indict-chinese-military-officers} accessed 20 November 2018.

[91]Grosrichard, *The Sultan's Court*, p. 11.

[92]Craig Timberg and Barton Gellman, 'NSA paying U.S. companies for access to communication networks', *Washington Post* (29 August 2013), available at: {https://www.washingtonpost.com/world/national-security/nsa-paying-us-companies-for-access-to-communications-networks/2013/08/29/5641a4b6-10c2-11e3-bdf6-e4fc677d94a1_story.html?utm_term=.c4c0c1721f43} accessed 20 November 2018.

https://doi.org/10.1017/S026021052000008X Published online by Cambridge University Press

be an internal power struggle, but can also – as anonymous NSA hackers reveal – be understood as being driven by a transgressive disregard for the publicly articulated norm of restraint.

On the surface, it is not very surprising that the former director of NSA/head of US Cyber Command Admiral Rogers sought to conduct active defence to try to infiltrate enemy networks rather than work with critical infrastructure companies to improve their defences.[93] The US Department of Homeland Security (DHS), not the NSA, is the primary responsible for safeguarding and raising the security levels in cyberspace within the United States. However, Rogers's predecessor, General Alexander, secretly lobbied *against* President Obama's attempt to strengthen the cyber responsibility and authority of DHS as it would weaken NSA in the internal power hierarchy of the United States.[94] Centralising US cyber power around the NSA/US Cyber Command seems to promise the freedom to – and ultimately the enjoyment associated with – excessively exploiting all the IT vulnerabilities available. Let me briefly illustrate the importance of the internal cyber hierarchy in the US government before pointing to how this relates to NSA's transgressive practices.

IT vulnerabilities, the mistakes and flaws made when programming, installing, and administrating IT systems, are generally perceived as the key to every major cyberattack. Without exploiting IT vulnerabilities, there would be no offensive cyber capabilities. This gives rise to a dilemma as many of the vulnerabilities the NSA/US Cyber Command exploit exist in products developed and maintained by US companies, such as Microsoft, and used by most Americans. The US government sometimes chooses *not* to publicise new IT vulnerabilities ('zero-days') that they identify.[95] A classified process – the Vulnerabilities Equities Process – has been put in place to clarify when to disclose and when to retain IT vulnerabilities.[96] In this process, the most important cyber entities in the US government assesses the IT vulnerabilities, and hence, the NSA, which is primarily concerned with exploitation, works internally to cement its position as the most important voice in making these decisions. The decisions to retain vulnerabilities always come with the risk of weakening the global cyber infrastructure and causing harm to companies and citizens, which the US cyber defence community, in public articulations, swears to protect. Yet, on closer look, several anonymous NSA hackers have revealed how the workings of the NSA is driven by a culture of transgression – of total disregard for a norm of restraint and public (both global and national) cybersecurity.

An illustrative example is linked with the worldwide 2017 ransomware incidents, WannaCry and NotPetya, that caused billions of dollars in damage. An anonymous NSA employee was quoted in the *Washington Post* defending the NSA's exploitation of the software vulnerability that enabled the attack. The employee notes that using the exploits had been 'like fishing with dynamite'.[97] In a Lacanian reading, 'fishing with dynamite' as a figure of speech for something easily accomplished makes better sense when compared to its literal meaning. Dynamite fishing is an illegal fishing practice highly destructive to the surrounding ecosystem. The statement can be interpreted as a slip of the tongue that reveals the transgressive desire of the US cyber defence community: implicitly, it is an inherently positive thing for the NSA to do what is illegal and damaging to the (cyber) environment – which is what China is publicly criticised for doing.

[93]Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York, NY: Simon & Schuster Paperbacks, 2016), pp. 281–2.

[94]Ibid.

[95]Michael Daniel, 'Heartbleed: Understanding when we disclose cyber vulnerabilities', *White House Blog* (28 April 2014), available at: {https://obamawhitehouse.archives.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities} accessed 20 November 2018.

[96]Ibid.

[97]Ellen Nakashima and Craig Timberg, 'NSA officials worried about the day its potent hacking tool would get loose. Then it did', *Washington Post* (16 May 2017), available at: {https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html?utm_term=.1a0da5176c99} accessed 20 November 2018.

https://doi.org/10.1017/S026021052000008X Published online by Cambridge University Press

In short, 'fishing with dynamite' exemplifies a perception of cyberspace present within the NSA that runs counter to the publicly articulated face of the US cyber defence community as a force of good that defends freedom and privacy.

Journalist Peter Maass, when interviewing another anonymous NSA hacker, who he calls the Lamb, provides another example of the US cyber defence's transgressive desire for enjoyment at the expense of both the US public as well as global cyber security. Maass cites the Lamb's dismissive attitude towards those outside the US cyber defence: the most technically sophisticated hacker conference in the world, DefCon, 'has basically nothing new to say'. And, the Lamb goes on to put the blame for NSA intrusions on the victims – 'if they were too dimwitted to protect themselves from hunters like him, it was their fault', Maass paraphrases the Lamb's point of view.[98]

The anonymous sources in the 2016 documentary on Stuxnet, *Zero Days*, echo this sentiment. The statements by one anonymous source cannot conceal the disdain for the public's fascination with Stuxnet – the worlds most sophisticated known malware that destroyed nuclear centrifuges in Iran – and their ignorance of much larger and more sophisticated cyber operation against Iran, NitroZeus. The voice brims with barely concealed pride as it explains the operation and the secretive, excessive preparation measures that transgress any form of restraint or principle of discrimination:

> We spend hundreds of millions maybe billions on it [the cyber operations to prepare for war with Iran]. … We built in attacks on Iran's command and control systems, so the Iranians couldn't talk to each other in a fight; we infiltrated their IADS – military air defence systems – so they couldn't shoot down our planes if we flew over; we also went after their civilian support systems: power grids, transportation, communications, financial systems. We were inside, waiting, watching, ready to disrupt, degrade, and destroy those systems with cyberattacks.[99]

These quotes paint a picture of the NSA as the place where one can enjoy the full possibilities provided by the insecurities of cyberspace. In contrast to the public promise of safeguarding an Internet for all, a key uniting element of the US cyber defence community is the transgressive disregard for providing cyber security to the general public.

Conclusion

The article contributes to the post-Snowden critical literature on security and surveillance. The existing contributions have done an important job mapping the various components of the complex material-discursive assemblage that make up today's global surveillance regime. Yet, the article suggests that the insights revealed by Edward Snowden and others about the transgressive behaviour of US cyber defence entities also reinvigorate what seems to have lost its appeal in studies of the mass surveillance, namely the traditional critical security study of how practices reproduce institutional identities and insecurities. The article follows the increasingly popular turn to Lacanian psychoanalysis in IR and security studies. Jacques Lacan and the contemporary interpretations by Slavoj Žižek pay particular attention to the constitutive role of transgression, and through their psychoanalytical lens, the article introduces a dual strategy for studying transgression in security studies: a symptomal reading and extracting the kernel of enjoyment.

In applying the dual Lacanian strategy to the study of the discrepancy between the official US cyber discourse of liberal values, restraint, and transparency and the secret, disavowed

[98]Peter Maass, 'The hunter – he was a hacker for the NSA and he was willing to talk. I was willing to listen', *The Intercept* (28 June 2016), available at: {https://theintercept.com/2016/06/28/he-was-a-hacker-for-the-nsa-and-he-was-willing-to-talk-i-was-willing-to-listen/} accessed 20 November 2018.

[99]Gibney (dir.), *Zero Days*, 1:45:25–1:46:25.

https://doi.org/10.1017/S026021052000008X Published online by Cambridge University Press

surveillance and cyber exploitation practices, the article makes two contributions. Theoretically, the case study contributes with an illustration of how to advance the study of transgression, not only among critical security scholars in general, but also – and primarily – among the Lacanian IR and security scholars, who have yet to engage thoroughly with this concept as that which ties together the fantasmatic image of a (lost) identity, the unconscious imperative to enjoy, and the object that prevents the fulfilment of the fantasy.

Empirically, the case study adds insights into one of the components of the global surveillance regime that has not to date received much attention in the critical and sociological studies on security and surveillance, namely the identification processes in the US defence and intelligence agencies that hold a key position in the complex surveillance assemblage. Here, the article shows that the representation of China as a top threat that rampantly enjoys transgressing the US promoted norms in cyberspace in pursuit of its narrow self-interest is not only a necessary discursive distinction that enables the fantasy of a US cyber defence identity by locating it out of reach. China is also a symptom that pushes internal tensions to the margin of that discourse and thereby enables the US cyber defence community to avoid confronting the anxiety-producing realisation that the social field it represents will never be able to fully deliver on its promise of national security and liberal values. Finally, the article argues that the representations of China also serve a purpose as the discursive place where the transgressive desire that arises from the laws and prohibitions that codify principles of restraint and cyber norms and by which the US cyber defence community officially abides, can take form and hold empirical content within the discourse. Thus, excessive Chinese transgressions are the US cyber defence community's own secret transgressive desire. And importantly, the US transgressive desire is lived out in secret as evident from leaked documents and anonymous sources. Such transgressions, through Lacanian lenses, provide the necessary partial enjoyment needed to sustain the US cyber defence community as well as the doctrine of restraint and cyber norm promotion that dominate the public discourse.

Acknowledgements. The author would like to thank Vibeke Schou Tjalve, Manni Crone, Helle Malmvig, Stefano Guzzini as well as several PhD students and postdoc researchers at the Danish Institute for International Studies who spent time commenting on earlier versions of the article. The editors of *Review of International Studies* and three anonymous reviewers also deserve special thanks for their very helpful and detailed comments and guidance.

Jeppe T. Jacobsen is an Assistant Professor at the Institute for Military Technology, Royal Danish Defence College. He previously worked at the Danish Institute for International Studies and as the cyber coordinator in the Ministry of Foreign Affairs of Denmark. He concentrates his current research on cyberspace operations and the international politics of cyberspace.

Cite this article: Jacobsen, J. T. 2020. Lacan in the US cyber defence: Between public discourse and transgressive practice. *Review of International Studies* **46**, 613–631. https://doi.org/10.1017/S026021052000008X

https://doi.org/10.1017/S026021052000008X Published online by Cambridge University Press