Neo and the 'Hacker Paradox': A Discussion on the Securitization of Cyberspace

https://www.e-ir.info/2022/02/24/neo-and-the-hacker-paradox-a-discussion-on-the-securitization-of-cyberspace/

BERNARDO BEIRIZ, FEB 24 2022

In the movie *The Matrix* (1999), Neo (codename of the character Thomas A. Anderson) leads a double life: during the day he works as a programmer in a software development company, but during the nights he reveals himself as a cybercriminal: a hacker.

In cybersecurity studies, references to movies like *The Matrix* may sound repetitive or even like the reproduction of stereotypes. The succinct description of Neo's dual identity, however, opens space for discussion about one of the elements that underlie this field of study: "the hacker paradox". I approach this idea from the standpoint of securitization theory and its developments in the field of International Relations, analysing the role of the hacker as identity and as a referent object in the securitization of cyberspace.

Before proceeding with the development of this concept, it is necessary to understand what cybersecurity is; in what ways can cyberspace be securitized? Myriam Dunn Cavelty and Thierry Balzacq define cybersecurity as "a multifaceted set of practices designed to protect networks, computers, programs, and data from attack, damage, or unauthorized access-in short, they are standardized practices by many different actors to make cyberspace (more) secure" (BALZACQ; CAVELTY, 2016, p. 183).

In what terms can we define the "hacker" identity from this definition of cybersecurity? The initial reaction tends to classify hackers as those who attempt against this multifaceted set of practices developed to protect networks; as those who break this set of "laws." In *The Matrix* (1999), the "agents" are part of an Artificial Intelligence program in the Matrix whose job is to keep it "safe". Promoting security in the Matrix involves fighting off cybercriminals like Neo, preventing hackers from altering the functioning of the set of networks, computers, and systems that make up the computer simulation that is the Matrix.

The presentation of Neo (or Thomas A. Anderson) as a programmer during the day, however, calls attention to a fundamental issue of cybersecurity, what I name "the hacker paradox." Leonie Maria Tanczer argues that "the supposed dichotomy and binary opposition of hacker versus IT and cybersecurity professionals" would clarify which actors would be responsible for doing "good" and which would be doing bad, defining what would be "safe" and what would be "insecure" (TANCZER, 2020, p. 6).

The paradox lies precisely in the coexistence of these two identities in the same individual. The characterization of a subject as a hacker or as an IT professional, therefore, has important implications for the securitization of cyberspace. This classification of certain individuals as "good" or "evil" can be exercised by the state by delimiting those who are "inside the law" and those who are "outside the law," but it can also occur based on the approval or disapproval of an external audience. Hacktivist groups like Anonymous, for example, can be ranked by public opinion at either end of the subjective scale of "good" or "evil. This classification depends on a recognition of the activities of "hacktivists" as "productive": they must fulfil collective requests or even generate public entertainment and engagement.

Understanding the classification of hackers as "good" or "evil" by public opinion is a philosophical-political-

sociological exercise beyond the scope of this paper. The results of the characterization of these hackers as “IT professionals” or as “computer hackers” by the state, however, influence the dynamics of cyberspace securitization and will be analyzed here.

The hacker and ontological insecurity in cyberspace

The NSA, one of the main national security agencies of the United States of America, is directly associated with the hiring of hackers, or “IT professionals” (depending on which classification is used). The use of the term hacker here is purposeful, as many of the individuals hired by agencies like the NSA have histories of criminal behaviour considering “practices designed to protect networks”; in light of the “laws” of cyberspace. The practice of hiring these individuals occurs for two reasons: firstly, the knowledge they possess is sorely needed to produce defence and attack mechanisms for the state in question; furthermore, these hackers/professionals navigate “grey waters”. In them, they are not necessarily protected by formally recognized laws, just as they will not necessarily be condemned by those same laws. They ultimately depend on the state’s classification: It is up to the state to determine whether these individuals are criminals or heroes, based on an area of law marked by subjective interpretations and judicial decisions or even a lack of laws and applicable jurisprudence.

But in what way is this possibility of characterization of the hacker as “good” or “evil” by the state crossed by the securitization of cyberspace? From here on, it becomes necessary to address some points about securitization theory.

The Copenhagen School, according to Lene Hansen and Helen Nissenbaum, understands security as a “speech act that securitizes, that is constitutes one or more referent objects, historically the nation or the state, as threatened to their physical or ideational survival and therefore in urgent need of protection” (HANSEN; NISSENBAUM, 2009, p. 1156). Securitization, in turn, especially in the field of cybersecurity, works by connecting different referent objects,” particularly by providing a link between those that do not explicitly invoke a bounded human collectively, such as ‘‘network’’ or ‘‘individual,’’ with those that do” HANSEN; NISSENBAUM, 2009, p. 1163).

Another way to understand securitization is from the descriptions provided by Didier Bigo and by Barry Buzan, Ole Waever and Jaap de Wilde. For Buzan, Waever and de Wilde, “securitization is the movement that takes politics beyond the established rules of the game and frames the issue either as a special kind of politics or as above politics.” (BUZAN; WAEVER; DE JAAP, 1998 p. 23). A “securitization movement,” therefore, must be able to convince an external audience (Ibid., p. 25), legitimizing the “securitization” of the issue, thus legitimizing its transfer to a field “above politics,” above practised rules.

Bigo presents security as being based on an intersubjective process (BIGO, 2008, p.125): “something” becomes presented to “someone” as a security issue. It is the practice of discourse that makes a certain issue a security issue and not necessarily the “real” existence of a threat: naming something as a threat can be a first “move of securitization” (Ibid., p. 125). Finally, to turn “something” (or someone), a referent object into a security issue, to securitize it, the securitizing agent must possess credentials, producing audience acceptance (Ibid., p. 128).

Cyberspace is constantly crossed by these dynamics of (in)securitization, following Bigo’s idea that security and insecurity can go together, that is, that the framing of one issue as security generates the role/position of insecurity for others. Understanding cyberspace as an ecosystem constituted by the coexistence between humans and “non-humans”, as a mélange between physical infrastructure, code, and human interaction, one can perceive the complexity of this space and the plurality of existing relations.

The hacker is an example of challenging the division between humans and non-humans. The engagement of the human with the “matter” in cyberspace from code, thus Neo’s action as a “computer hacker,” often confuses “human” actions with failure: when an information system stops working, one might initially attribute this to a “processing failure,” inherent in the operating logic of the technology itself, when in reality it is connected to the deliberate action of a hacker.

This feature reinforces the notion of cyberspace as a dangerous environment in which one cannot be certain. Moreover, some actions of "ordinary" users can facilitate the action of cybercriminals, so that the former are also transported into the "hacker paradox": depending on their actions, endowed or not with intentionality (something that, especially in the digital sphere, cannot be verified), ordinary users can be classified as threats, resulting in a constant state of being characterized as "potential threats" (HANSEN; NISSENBAUM, 2009, p. 1166) – which picks up on an idea of constant state of alert developed by the United States in the context of the war on terror. In an interesting passage from Hansen and Nissembaum's text, the authors state that just "as in discourses about epidemics and contagion, cyber insecurities are generated by individuals behaving irresponsibly, thus compromising the health of the whole" (Ibid., p. 1166).

In a bold step, I claim that, in short, there is an inherent ontological insecurity in information systems. The first way to see this insecurity is in the "hacker paradox" described earlier. Marco A. Vieira argues that "in the conventional sense, therefore, ontological security relates to the individuals' psychological ability to sustain a coherent and continuous sense of who they are" (VIEIRA, 2017, p. 6). Considering the logic of (in)securitization described by Buzan, Waever, de Wilde, and Bigo, the dual identity assigned to the hacker/IT professional produces a constant threat, to be determined by the state (as well as by other "private" securitizing agents, such as private cybersecurity agencies). This process, therefore, leads to the erosion of precisely this psychological capacity of individuals to have a sense of their identity.

The differentiation between "us" and "others", characterizing referential objects as either "security" or "insecurity" is lost the moment hackers/IT professionals are simultaneously part of the "us" and the "others". The "hacker paradox," therefore, reinforces the logic of (in)securitization by blurring the differentiation of identities, rendering all those who are responsible for developing and promoting "security" on networks as potential threats.

Another way to understand the ontological insecurity of informational systems is to pay attention to the functioning of cyberspace and the "quasi-agency" of matter. On the functioning of digital systems, it is necessary to understand it as based on the mélange described earlier: there are several points of "failure" at the intersection between human interaction, code, and physical infrastructure. "Threats arise from software as well as hardware failures and cannot be corrected from improved digital technology and programming" (HANSEN; NISSENBAUM, 2009, p. 1160). Cyberspace is crossed by systemic threats, generated by the unpredictability of the action of computers and information systems (Ibid., p. 1160). These failures, however, when occurring in a system that encompasses both the "real," the analogue, the concrete, and the digital, can generate potentially dangerous situations for the information systems themselves or for the physical and human systems in which they are embedded (Ibid., p. 1160).

Neo is able to manipulate the Matrix through a specific form of hacking, however, being directly connected to this "cyber system", he also suffers from the consequences of what happens in the Matrix. In other words, and using more concrete examples, attacks such as Stuxnet (which interfered with the operation of Iranian nuclear power plants) or ransomware attacks responsible for the malfunctioning of hospitals, show the human vulnerability to the multiple and infinite possible failures that arise in digital systems. Fostering a relationship of dependency is, in a way, accepting to deal with an insecurity that cannot be solved, since it does not reside only in the action of the humans that make up the mélange, but in the "autonomous" interaction of the machines themselves.

An indispensable opportunity now arises for the discussion of the "quasi-agency" of matter described by science and technology studies. A first, the more objective approach is taken by James Breassett and Nick Vaughan-Williams, based on the idea of resilience attributed to the "CNI2000 Intruder Detection System (IDS)". This system, according to the authors, would be able to autonomously determine whether a threat is real, not depending on human interpretation. According to them, the system would be "able to perform its own (in)securitization moves" (BRASSET; VAUGHAN-WILLIAMS, 2015, p. 41). The CNI2000 IDS would therefore be a clear example of how there is "a belief in and a dependence on the agentic capacity of protection technologies to protect themselves: to ensure that resilience infrastructures remain resilient" (Ibid., p. 42).

The agency of the CNI2000 IDS is explicit and easily identified, as it occurs from automation, from decision-making by machines, replacing and mimicking human action. The description of the functioning of cyberspace conducted

earlier, however, enables a more interesting discussion. I argue that in cyberspace, in the mélange that constitutes it, each “unit of matter”, be it a mouse, a line of code, a set of servers or a click made by a “human”, is endowed with agency: all these “units of matter” are capable of causing difference, this being the definition of agency for authors like Bruno Latour (but also resembling Anthony Giddens’ idea that agency is the ability to interfere with structure). The agency of hackers, therefore, is indisputable, since they, directly and indirectly, possess the ability to interfere with digital systems in various ways.

Thinking about algorithms and their relationship to cyber (in)security, it is possible to interpret them as “ethical-political arrangements of values, assumptions, and propositions about the world” (AMOORE, 2020, p. 6). These arrangements, however, are technological tools that “need to be embedded in a combination of human and/or machine to be executed” (WILCOX, 2016, p. 16). The need for embedding is a fundamental part of the “cyborg” connection established between the “digital” and the “human,” therefore, of the cyber ecosystem. Hackers participate in this cyborg embodying movement: hackers are the subjects of this embedment.

The embedding and the execution of code, crossing the boundaries between human and non-human, pervade the logic of securitization and must also be thought of in ethical and philosophical terms: the deliberate production of mechanisms capable of performing their own “(in)securitization moves” constitutes the effective and indisputable implementation of agency for these technological entities. Although both “matter units” and “humans” can simultaneously “possess agency,” the production of these autonomous/automated mechanisms raises the question: is this not part of a process of replacing human agency with technological agency? In other words, does the ability to cause difference described by Latour remain the same while not even the (in)securitization movements are performed by “humans”? Does this alter the hacker “identity” or the “hacker paradox”? These are open-ended questions, for which there are no simple answers.

Conclusion

Cyberspace, therefore, seen as an ecosystem that encompasses “humans” and “non-humans”, becomes the ideal environment for the proliferation of threats, reinforcing the multiplication of (in)securitization movements, whether produced by “humans” or by “matter units” (based on a broad interpretation of agency). The hacker, as an identity, threat, and referent object of these (in)securitization movements, is subject to constant instability, as he simultaneously occupies the side of “us” and “them” in the production of security and insecurity. I believe that this movement occurs not only in the external perception and interpretation about hackers; that this instability is not only present in the view of (in)securitizing agents, but also internally. Like Neo in *The Matrix*, given a context of instability, in which the subject is not able to be certain about his “side,” it is possible that an “internal doubt” arises for hackers about their position in these dynamics. The “hacker paradox” in this context takes on both an external and internal face, an idea that has yet to be explored.

This instability and the unpredictability and interconnectivity characteristics of cyberspace reinforce the (in)securitization movements, as it makes all components of cyberspace possible threats: from a lay user in matters of cybersecurity who acts in a “dangerous” or “unsafe” manner when downloading music from an “untrusted” website to a particular hardware component of an intrusion detection system that unpredictably fails at the moment of an intrusion, all are endowed with agency in cybersecurity and thus portrayed as possible threats.

Security in cyberspace should not be ignored. Ensuring the proper functioning of information systems goes beyond a rhetorical exercise, as the mélange of the cyber ecosystem shows us the dependence of human life on digital infrastructure. These discussions, however, must be able to coordinate (in)securitization practices sparingly, since these may be responsible for characterizing cyberspace as solely a “security” issue, which it is not. Attention should also be paid to the replacement of “human” agency by “technological” agency, achieved through the development of automated systems, capable of defining their own (in)securitization movements.

References

AMOORE, Louise. Introduction: Politics and Ethics in the Age of Algorithms. In: Ethics in the Age of Algorithms:

Algorithms and the Attributes of Ourselves and Others. Durham and London: Duke University Press, 2020.

BALZACQ, Thierry; DUNN CAVELTY, Myriam. An actor-network theory for cybersecurity. European Journal of International Security, Vol. 1, part 2, pp. 176-198. 2016.

BIGO, Didier. International Political Sociology. In: Williams, Paul (ed.). Security studies: an introduction. New York: Routledge, 2008, pp. 116-129.

BUZAN, Barry; WAEVER, Ole; DE WILDE, Japp. Security: A New Framework for Analysis. London: Lynne Rienner Publishers, 1998. Chapter 1 (pp. 1-20) and Chapter 2 (pp. 21-47).

BRASSET, James; VAUGHAN-WILLIAMS, Nick. Security and the performative politics of resilience: Critical infrastructure protection and humanitarian emergency preparedness. Security Dialogue 46(1), pp. 32-50, 2015.

DUNN CAVELTY, Myriam. The materiality of cyber threats: logics of securitization in popular visual culture. Critical Studies on Security 7 (2), p. 138-151, 2019.

DUNN CAVELTY, Myriam; WENGER, Andreas. Cybersecurity meets security policy: Complex technology, fragmented policy, and networked science. Contemporary Security Policy 41 (1), pp. 5-32, 2020.

HANSEN, Lene; NISSENBAUM, Helen. Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly 53, p. 1155-1175, 2009.

HUREL, Louise Marie. Cybersecurity and Internet Governance: two competing fields? Thesis (bachelor's degree in International Relations) – Institute of International Relations, Pontifical Catholic University of Rio de Janeiro. Rio de Janeiro, 2016.

LOBATO, Luísa Cruz; KENKEL, Kai Michael. Discourses on the securitization of cyberspace in Brazil and the United States. Brazilian Journal of International Politics 58 (2): 23-43, 2015.

SHIRES, James. Cyber-noir: cybersecurity and popular culture. Contemporary Security Policy Vol. 41, no. 1, p. 82-107, 2020.

TANCZER, L. M. 50 shades of hacking: How actors in the IT and cybersecurity industry perceive good, bad, and former hackers. Contemporary Security Policy, 41(1), 108-128. 2020.

VIEIRA, Marco A. "(Re-)imagining the 'Self' of Ontological Security: The Case of Brazil's Ambivalent Postcolonial Subjectivity". Millennium: Journal of International Studies, DOI: 10.1177/0305829817741255, 2017.

WILCOX, Lauren. Embedding algorithmic warfare: Gender, race, and the posthuman in drone warfare. Security Dialogue 48(1), p. 11-28, 2017.