Deterritorializing cyber security and warfare in Palestine: Hackers,sovereignty, and the National Cyberspace as normative

Cristiano, F.

CyberOrient, Vol. 13, Iss. 1, 2019, pp. 28–42

Deterritorializing Cyber Security and Warfare in Palestine: Hackers, Sovereignty, and the National Cyberspace as Normative

Fabio Cristiano

Leiden University

Abstract:

Cybersecurity strategies operate on the normative assumption that national cyberspace mirrors a country's territorial sovereignty. Its protection commonly entails practices of bordering through infrastructural control and service delivery, as well as the policing of data circulation and user mobility. In a context characterized by profound territorial fragmentation, such as the Occupied Palestinian Territory (OPT),[1] equating national cyberspace with national territory proves to be reductive. This article explores how different cybersecurity strategies – implemented by the Israeli government, the Palestinian Authority, and Hamas – intersect and produce a cyberspace characterized by territorial annexation, occupation, and blockade. Drawing on this analysis, it then employs the conceptual prism of (de-)–(re-) territorialization to reflect on how these strategies, as well as those of Palestinian hackers, articulate territoriality beyond the normativity of national cyberspace.

Keywords:

national cyberspace, cybersecurity, cyber warfare, securitization, Palestine

Introduction

Overlooking the Israeli checkpoint in Qalandyia, a Palestinian village between Jerusalem and Ramallah in the West Bank, a graffiti dominates the grey surface of the adjacent separation wall with the computer command *ctrl+alt+del*, written in giant capital letters.[2] Typically used to terminate an unresponsive task, the light-blue painted keyboard shortcut figuratively portraits the wall itself as a failed process that needs to be forcibly terminated. At the same time, the graffitied command also traces a continuity between spatial and cyber closures for Palestinians.

Corresponding author: Fabio Cristiano, Leiden University, 2501 EE, Hague, The Netherlands. E-mail: f.cristiano@fgga.leidenuniv.nl

National cybersecurity policies, as well as offensive and defensive cyber warfare, are commonly inspired by a similar perceived continuity: the spatial correspondence between national territory and sovereignty in cyberspace. Assigning traditional territorial qualities to cyberspace, national authorities envision its protection through physical bordering and different approaches to the ordering of mobilities for both data and users.[3] Regulating extent and modes of data circulation and user mobility, cybersecurity purports to order and secure the *national cyberspace* on the basis of its congruence with a country's territory.[4]

For its territorial fragmentation and diverse regimes regulating mobility, the case of the Occupied Palestinian Territory offers a unique perspective to reflect on the territorial qualities of cyberspace and its securitization. On one hand, territorial sovereignty represents, in fact, the ultimate raison d'être of the Israeli–Palestinian conflict; on the other, multiple and shifting regimes of mobility compile the complex grammar of the distributed system of control over the biopolitical life of the Palestinians. These regimes constitute the result of different degrees of Israeli territorial control: annexation of East Jerusalem, occupation of the West Bank, and blockade of the Gaza Strip.

This article explores how Israeli and Palestinian strategies intersect, enact, and disrupt territorial control over cyberspace, and whether these are consistent with the current fragmentation of the Palestinian territory. Whereas Israel's absolute control over infrastructural networks configures foremost as a direct practice of territorial bordering, recent legislations of the Palestinian Authority (PA) operate on territoriality in less direct forms. Imposing severe limitations on user mobility and data circulation, these measures ultimately replicate PA's security cooperation with Israel also in cyberspace.

Furthermore, this article advances a critique of a "static" territorial understanding of sovereignty in cyberspace through the analysis of offensive operations conducted by Palestinian hackers. Inspired by theoretical works on (de-)–(re-)territorialization (Deleuze and Guattari

1988; Deleuze and Guattari 2000; Foucault 2007), the analysis of these hacking operations further indicates how the territorial articulation of cyberspace does not linearly stem from national sovereignty. Rather, it encompasses different relational moments of becoming sovereign: whereas de-territorialization pertains to the moment in which established norms are disarticulated, re-territorialization refers to redo the undone (Petersen 2014; Waldenfels 2004).

In this light, Palestinian hacking operations can be understood as moments of "becoming sovereign" through (de-)–(re-)territorialization to the same extent of national policies and strategies. Furthermore, the lack of univocal spatial boundaries in cyberspace – and a necessarily distributed approach to security – empowers Palestinian hackers to overcome the technological obsolescence imposed on them through creative forms of social engineering and manipulation (Bullée et al. 2018) As these define the territoriality of cyberspace as a function of how users and data move, this article ultimately interrogates the normative assumption that a national cyberspace reproduces tout court its corresponding national territory.

National cyberspace and national territory

In contrast with cyber-utopianist visions of a borderless Internet, national security and defense policies contributed to the current disintegration and fragmentation of cyberspace into national subdivisions (Mueller 2017; Mueller 2010; Morozov 2011). These "compartments" are thought to possess spatial and territorial characteristics that are equivalent to those of a sovereign country (Wu 1997; Mueller 2002). In classical realist terms, a delimited, continuous, and internationally recognized territory constitutes, in fact, an essential element to define national sovereignty. It is thus primarily through physical bordering that a space becomes a territory. Besides legislative implications, the bordering of a specific space creates two different spatial realities: an inside and an outside.[5] In addition to fulfilling a spatial function, the delimitation of a territory operates then through a normative logic of inclusion–exclusion, peculiar to the ordering function that a territory plays in relation to identity.

At a basic level, national authorities enact the territorial delimitation of their national cyberspace through control over infrastructural elements of the network: the backbone, fiber cables, servers, switches, et cetera (DeNardis and Musiani 2016). National control over the backbone – also referred to as "core network" – constitutes the primary feature that sets forth national sovereignty in cyberspace. This public core (Broeders 2015) comprises a series of principal data routes and computer networks that, gathered and administered by a central authority, determine control of the physical components of the Internet network, and thus its fundamental territoriality. At the same time, with responsibilities for the security of cyberspace distributed to a variety of actors other than the state,[6] local nodes and ramifications constitute the ultimate terrains where territoriality, and thus sovereignty, unfold (Broeders 2017).

In contravention of Art.36/3 of Oslo II (1995) – that unambiguously declares the PA's right to infrastructural autonomy – Israeli authorities currently control the Internet backbone and the infrastructural network for the entire 1948 territory (AbuShanab 2019). From an infrastructural perspective, Israel's absolute control of the "bare metal" elements of cyberspace in fact exceeds its legitimate territorial boundaries, and thus reproduces the illegal territorialities of annexation, occupation, and blockade over the Palestinian territory.

In 1967, in the aftermath of the Six-Day War, Israel annexed Palestinian areas east of the armistice line (the Green Line). Advancing this annexation through concrete bordering, in the early 2000s, the Israeli government put "facts on the ground" by erecting the contested separation wall. Deviating its path from the internationally-recognized border (the Green Line), the wall concretely annexes East Jerusalem, thus detaching the designated Palestinian capital from the West Bank. The territorial annexation of East Jerusalem also pertains to cyberspace. Besides controlling the Internet backbone, the Israeli annexation unfolds through the denial of service provision, with a ban outlawing Palestinian Internet service providers (ISPs) and mobile carriers from delivering and commercializing Internet service in the city (AbuShanab 2018). Operating through an archetypal logic of exceptionalism[7] – that is the sovereign suspension of agreed norms

and political freedoms – Israeli policies ultimately purport to detach the Palestinian city also from its national cyberspace.

Whereas cyberspace in East Jerusalem undergoes complete annexation – in line with the Zionist imaginary of a unified Jewish city[8] – the Israeli occupation of the West Bank translates into cyberspace through less direct forms of territorial control. The PA holds, in fact, the responsibility for Internet governance and service provision across the Palestinian areas of the West Bank. However, the Israeli absolute control of the infrastructure means that Palestinian ISPs depend on their Israeli homologs to supply a second-hand, and expensive, Internet connection across the territory. A 2016 World Bank report indicates that, besides detaining full control on the core network, Israeli authorities regularly block the import of ICT equipment and technologies towards the Palestinian controlled areas of the West Bank (AbuShanab 2019). At the very least, one should ask whether national sovereignty in cyberspace can ever be attained in the absence of infrastructural autonomy.

With Oslo I (1993) granting Israel jurisdiction over Area C (presently ca 61 percent of the West Bank), Palestinian Internet operators require multiple authorizations for transporting or installing technologies in the area. Citing security concerns, the Israeli Civil Administration (ICA) regularly turns them down, while Israeli providers supply Internet connection and mobile services to illegal Jewish settlements in Area C. As settler presence in the West Bank has quadrupled since 1993 (EEAS 2019) – despite several peace agreements establishing an official freeze on their expansion – Israeli ISPs improved and expanded the infrastructural network needed to serve the growing settler community (across the West Bank and East Jerusalem). Due to this, Palestinians in Area C need to roam on Israeli frequencies to access mobile Internet, commonly opting to subscribe to one of the Israeli operators (Niksic et al. 2014).

In absence of absolute control over service provision, the Israeli occupation translates in cyberspace through measures of less concrete and direct bordering. Whereas the annexation of East Jerusalem in cyberspace marks

a continuity with the erection of the separation wall, the occupation of cyberspace in the West Bank hinders service delivery in ways that are reminiscent of Israeli roadblocks, (flying) checkpoints, and its Kafkaesque permit system (Berda 2017).

Internet governance in the Gaza Strip functions through a setup similar to the one in the West Bank. Relying on the Israeli core network, Palestinian ISPs deliver a secondhand service across the Hamas-governed territory (Tawil-Souri 2012). Since 2006, however, following Hamas' success in the Palestinian elections, Israel has imposed a territorial blockade on the Gaza Strip. The Israeli illegal blockade severely limits the mobility of goods and people, thus further isolating the area from the rest of the Palestinian territory (Erakat 2012). As a result, Gaza currently relies on Israel even for the provision of basic services such as electricity, water, and sewage treatment (World Bank 2019). Likewise, Israeli authorities control the entire telecommunication system, including wired and wireless Internet. For this reason, Palestinian ISPs need permits to access the Gaza Strip in order to perform infrastructural maintenance, but these are regularly turned down (Abou Jalal 2017). Furthermore, Israeli bombardments on ICTs, as well as regular power cuts, further compromise the infrastructure and service delivery (Weinthal and Sowers 2019). As territorial blockade extends to bandwidth, spectrum, and frequency allocation, Israeli measures force Gaza into a state of technological obsolescence and dependency. Through infrastructural control and cybersecurity, Israel upholds territorial sovereignty over Gaza's seized cyberspace.[9]

Cybersecurity as territorial bordering

Israel currently organizes its national cybersecurity in the light of a centralized governance model. Since 2017, a single unit – the National Cyber Directorate (NCD) – holds responsibility for the protection of both civilian and military nodes of the national cyberspace, thus conflating security and defense strategies. Besides infrastructural control and cyber defense, the Israeli territorial control over Palestinian cyberspace heavily relies on cybersecurity measures that are conventionally enforced in domestic contexts.

In addition to traditional cyber espionage, Israeli security forces recur to the algorithmic parsing of Palestinian online content as part of predictive policing and pre-crimes. This flagging primarily focuses on social media, wherein the automatic scanning examines contents to detect data of alleged security relevance (Cristiano 2018). Evidence indicates that – besides a pool of blacklisted Arabic words such as *freedom*, *martyr*, *Al Aqsa*, et cetera – the algorithms intercept status updates and content flagged solely for their political connotation and indicating no warning of violence of any kind (AbuShanab 2018). These measures target Palestinians across the 1948 territory as well the international diaspora, thus superseding any rationale of national and territorial sovereignty.

The PA and Hamas enforce cybersecurity strategies that further hinder mobility in cyberspace for the Palestinians. In 2018, the PA approved a controversial cybercrime law: operating through two focal aspects – content management and access regulation – this legislation purports to protect "national unity" and "social harmony" (Article 51) across its national cyberspace. In practice, it urges Palestinian ISPs and hosting services to take down those websites, blogs, and online content that PA and its security agencies flag as a threat to national security or values (Abdeen 2018). Citing concerns to national security, the legislation also outlaws connection via alternative routes (Article 31) such as VPNs, mesh networking, I2P, and the like. Banning these methods reenacts Israeli territorial control as it purports to constrain traffic along the occupied national network. In other words, outlawing alternative routes ultimately reterritorializes potential Palestinian "escapes" into a preserved spatial status quo (Arafeh et al. 2015).

Conversely, Hamas government retains marginal power over its national cyberspace. The absence of locally-controlled infrastructures and service provision severely hinders Gaza's ability to develop its own strategy of cybersecurity. In 2012, Hamas tried in vain to regain sovereignty over its cyberspace by introducing a ban on the use of Israeli connection services. With little or no authority over infrastructure and service delivery, Hamas' cybersecurity unfolds by tightening control over endusers and local nodes of the network. Its security forces employ in fact extensive surveillance to

motivate the arrest and prosecution of political opponents or dissidents (AbuShanab 2019). These same techniques are used for policing compliance to Islamic precepts: having enforced a ban on "immoral websites", security forces regularly raid Internet cafes to monitor how users roam online (AbuShanab 2019).

Hacking as (de-)–(re-)territorialization

The previous sections illustrate how different cybersecurity strategies function as devices of territorialization for (fragments of) Palestinian cyberspace and corroborate evidence of a strong correspondence between national cyberspace and national territory. While operating in a context defined by territorial sovereignty, these national strategies construct and reinforce territorial ordering in cyberspace on their own. In this sense, cybersecurity articulates and orders the boundaries of sovereignty through the creation of an outside "other".

Palestinian hackers – autonomous or operating as a cyber wing for a political faction (Hamas, PFLP, Jihadists, etc.) – participate in this articulation of sovereignty through offensive techniques, targeting Israeli cyberspace on both its military and civilian nodes. These include both intrusive strategies for gathering intelligence (spear-phishing, spyware, ransomware, etc.) as well as disruptive ones (distributed denial-of-service attacks, takedowns, redirects, defacements, etc.) (Rudner 2013). Whereas these attacks intensify in concomitance with violent escalations, they constitute an immanent feature of regional cyber warfare; despite vastly asymmetric cyber potentials in Israel–Palestine, these campaigns have proved a great asset for Palestinian groups.

These operations commonly feature somewhat unsophisticated coding, but advanced social hacking techniques, thus crediting their success to well-designed baits tricking Israeli users into allowing passage for malicious contents. Context-tailored emails, deceitful apps (gaming, dating, news, etc.) and fake social media links specifically target military and governmental personnel (IDF 2017). In 2018, Palestinian hackers

implanted a spyware into an app mimicking the Red Alert, a service that warns Israeli users in the event of imminent rocket attacks from Gaza. This technique exploited the logic of ubiquitous securitization: attacking through a software that warns about attacks (ClearSky 2018).

Besides low-tech hacking, Palestinian cyber operations have at times shown unanticipated levels of sophistication and effectiveness, in spite of the obsolete infrastructures across the territory. In 2013, for example, the cyber wing of the Izz ad-Din al-Qassam Brigades (IADAQ) took control of a series of Israeli websites and servers through a technique of direct de-territorialization. Whereas not unique in terms of outcomes – as thousands of Israeli websites have been taken down or defaced by Palestinians in the last fifteen years – this operation appeared at the time unique for the sophisticated design of Distributed Denial-of-Service (DDoS).[10] Palestinian hackers coded a programming language that, operating on the controlled zombie-network, allowed them to access a larger bandwidth needed for carrying out the attack. Through the manipulation of codes, hackers successfully e the bandwidth available to them.

On other occasions, Palestinian hackers combine complex operations with the aforementioned social hacking techniques. One of Israel's basic cybersecurity provisions consists of blocking the mobility of all data coming from the Gaza Strip in order to prevent them from reaching its network endpoints (AbuShanab 2019). In these conditions, the success of cyberattacks launched from Gaza primarily depends on the ability to circumvent this territorial block. In 2015, Gaza-based hackers launched a massive spear-phishing attack on Israeli cyberspace: bypassing the blockade, the operation compromised and accessed databases belonging to public offices, military departments, private companies, and individual users (Trend Micro Threat Research Team 2015). Palestinian hackers leveraged these attacks – referred to as Operation Arid Viper – on servers based in Germany. Through this expedient, the Israeli cyber dome failed to detect them as originating from Gaza and thus approved their passage. On the other hand, the attack employed diverse bait contents for different targets, in line with one of the social hacking precepts: vulnerability

resides in users' behavior and choices, to a degree uncontrollable for national cybersecurity and its normative understanding of sovereignty.

Conclusions

In August 2017, a 64-year-old Palestinian man, resident of Isawiya in East Jerusalem, recounted to me his frustration over a recent economic loss. A few days earlier, a cyberattack had irremediably compromised his company website and databases. Together with the message "Freedom to Palestine", the defacing image of an armed cyborg holding a Palestinian flag was now peeping out the homepage of his family business website. A historical advocate of the Palestinian cause, and member of the Palestinian Liberation Organization (PLO), had himself fallen victim of hackers targeting Israeli cyberspace in solidarity with Palestine.

These hackers apparently acted on the common creed that domain names are a sufficient indication of territorial identification: attacking websites hosted on the domain *.il* would equate to attacking Israel. In general terms, country code top-level domains (ccTLDs) are indeed reserved for sovereign polities and formally extend the boundaries of national jurisdictions to cyberspace (Mueller and Badiei 2017). Together with national control on core networks, this conventional arrangement marks a linear continuity between national cyberspace and national territory. As argued throughout this article, the complex spatial realities across the Palestinian territory demonstrate the issues associated with this assumption.

Above all, the architecture of cyberspace assigns extensive control functions to its network nodes (van den Berg and Keymolen 2017). Unique to this architectural structure, the resilience of the system allows for the rerouting of data traffic through alternative routes in case of closure (Ruiz and Barnett 2015). Network nodes are thus part of how territories are articulated in cyberspace in ways that are independent of a static correspondence with the national territory. Besides infrastructural control, this article has argued that (de)–(re)territorialization in cyberspace occurs primarily through the ordering, and disordering, of data circulation and user mobility.

Israeli and Palestinian national cybersecurity strategies, as well as hacking operations, operate in fact in light of a spatial imaginary that, while being consistent to respective national imaginaries, moves away from (legitimate) territorial sovereignty. By articulating an exception, this very estrangement creates a sovereign space. In these terms, cybersecurity strategies (or the hacking thereof) can do more than enacting a preimagined territory: it can create a new one.

References

Abdeen, Isam. 2018. *Measures Taken by Al-Haq to Counter the Law by Decree on Cybercrimes*. Ramallah: Al-Haq Law for Human Rights.

Abou Jalal, Rasha. 2017. "How Gazans are dealing with Internet crisis." *Al-Monitor*, July 9, 2017, https://www.al-monitor.com/pulse/originals/2017/07/gaza-power-cuts-electricity-crisis-internet-israel.html.

AbuShanab, Anan. 2018. *Connection Interrupted: Israel's Control of the Palestinian ICT Infrastructure and Its Impact on Digital Rights*. Haifa: 7amleh - The Arab Center for the Advancement of Social Media.

AbuShanab, Anan 2019. *Hashtag Palestine 2018: An Overview of Digital Rights Abuses of Palestinians*. Haifa: 7amleh - The Arab Center for the Advancement of Social Media.

Agamben, Giorgio. 2005. *State of Exception*. Translated by Kevin Attell. Chicago: University of Chicago Press.

Arafeh Nur, Sam Bahour, and Abdullah Wassim. 2015. "ICT: The Shackled Engine of Palestine's Development." *Al-Shabaka*, November 9, 2015, https://al-shabaka.org/briefs/ict-the-shackled-engine-of-palestines-development/.

Berda, Yael. 2017. *Living emergency: Israel's permit regime in the occupied West Bank*. Palo Alto: Stanford University Press.

Broeders, Dennis. 2015. *The public core of the Internet*. Amsterdam: Amsterdam University Press.

Broeders, Dennis. 2017. "Aligning the international protection of 'the public core of the Internet' with state sovereignty and national security." *Journal of Cyber Policy* 2, no. 3: 366–376.

Bullée Jan-Willem H., Lorena Montoya, Wolter Pieters, Marianne Junger, and Pieter Hartel. 2018. "On the anatomy of social engineering attacks – A literature-based dissection of successful attacks." *Journal of Investigative Psychology and Offender Profiling* 15, no. 1: 20–45.

ClearSky. 2018. *Infrastructure and Samples of Hamas' Android Malware Targeting Israeli Soldiers*. Cambridge: Clearsky Security Ltd.

Cohen, Julie E. 2007. "Cyberspace As/And Space." *Georgetown Public Law and Legal Theory*, Research paper no. 898260.

Cristiano, Fabio, and Emilio Distretti. 2017. "Along the Lines of the Occupation: Playing at Diminished Reality in East Jerusalem." *Conflict and Society* 3, no. 1: 130– 143.

Cristiano, Fabio. 2018. "Internet Access as Human Right: A Dystopian Critique from the Occupied Palestinian Territory." In *Human Rights as Battlefields*, edited by Blouin-Genest Gabriel, Marie-Christine Doran, and Sylvie Piquerot, 178–201. Basingstoke: Palgrave Macmillan.

Deleuze, Gilles, and Félix Guattari. 1988. *A Thousand Plateaus: Capitalism and Schizophrenia*. London: Bloomsbury Publishing.

Deleuze, Gilles, and Félix Guattari. 2000. *Anti-Oedipus: Capitalism and Schizophrenia*. Minneapolis: University of Minnesota Press.

DeNardis, Laura, and Francesca Musiani. 2016. "Governance by Infrastructure." In *The Turn to Infrastructure in Internet Governance*, edited by Musiani, Francesca, Derrick L. Cogburn, Laura DeNardis, and Nanette S. Levinson, 3–35. London: Palgrave Macmillan.

Erakat, Noura. 2012. "It's Not Wrong, It's Illegal: Situating the Gaza Blockade Between International Law and the UN Response." *UCLA Journal of Islamic and Near Eastern Law* 11, no. 37: 40–83.

Foucault, Michel. 2007. *Security, territory, population: lectures at the Collège de France, 1977–78*. New York City: Springer.

IDF. 2017. "Hamas Uses Fake Facebook Profiles to Target Israeli Soldiers." The Israel Defense Forces, February 5, 2017, https://www.idf.il/en/articles/hamas/hamas-uses-fake-facebook-profiles-to-target-israeli-soldiers/.

Kostopoulos, George. 2012. *Cyberspace and Cybersecurity*. London: CRC Press.

Minelli, Filippo. 2019. "PROJECTS." Filippo Minelli Studio, accessed December 15, 2019, http://www.filippominelli.com/projects/.

Morozov, Evgeny. 2011. *The Net Delusion: The Dark Side of Internet Freedom*. New York City: Public Affairs.

Mueller, Milton. 2002. *Ruling the Root: Internet Governance and the Taming of Cyberspace*. Cambridge: MIT Press.

Mueller, Milton. 2010. *Networks and States. The global politics of Internet governance*. Cambridge: MIT Press.

Mueller, Milton. 2017. *Will the Internet Fragment?* Cambridge: Polity Press.

Mueller, Milton, and Farzaneh Badiei. 2017. "Governing Internet Territory: ICANN, Sovereignty Claims, Property Rights and Country Code Top Level Domain Names." *Columbia Science & Technology Law Review* 18, no. 1: 435–515.

Niksic, Orhan, Nur Nasser Eddin, and Massimiliano Cali. 2014. *Area C and the future of the Palestinian economy*. Washington, DC: The World Bank.

Oslo I. 1993. *Declaration of Principles on Interim Self-Government Arrangements*. Washington, DC. September, 13, 1993.

Oslo II. 1995. *Interim Agreement on the West Bank and the Gaza Strip*. Washington, DC. September, 28, 1995.

Petersen, Gregers. 2014. "Freifunk: When Technology and Politics Assemble into Subversion." In *Subversion, Conversion, Development: Cross-Cultural Knowledge Exchange and the Politics of Design*, edited by Leach James and Lee Wilson, 39–56. Cambridge: MIT Press.

Rudner, Martin. 2013. "Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge." *International Journal of Intelligence and CounterIntelligence* 26, no. 3: 453–481.

Ruiz Jeanette B. and George A. Barnett. 2015. "Who owns the international Internet networks?" *The Journal of International Communication* 21, no. 1: 38–57.

Tawil-Souri, Helga. 2012. "Digital Occupation: Gaza's High-Tech Enclosure." *Journal of Palestine Studies* 41, no. 2: 27–43.

Trend Micro Threat Research Team. 2015. *Operation Arid Viper: Bypassing the Iron Dome*. Shibuya City: Trend Micro Inc.

van den Berg, Bibi, and Esther Keymolen. 2017. "Regulating security on the Internet: control versus trust." *International Review of Law, Computers & Technology* 31, no. 2: 188–205.

Waldenfels, Bernhard. 2004. "The Boundaries of Orders," *Philosophica* 73, no. 1: 71–86.

Weinthal, Erika, and Jeannie Sowers. 2019. "Targeting infrastructure and livelihoods in the West Bank and Gaza." *International Affairs* 95, no. 2: 319–340.

World Bank. 2019. *Economic Monitoring Report to the Ad Hoc Liaison Committee*. Washington, D.C.: World Bank Group.

Wu, T. S. 1997. "Cyberspace Sovereignty: The Internet and the International System." *Harvard Journal of Law & Technology* 10, no. 3: 647–666.

Notes

[1] In line with the conventional use of the United Nations, conventional this article employs the definitions Palestine, Occupied Palestinian Territory, Palestinian territory to refer interchangeably to the recognized Palestinian territory in its entirety: East Jerusalem, West Bank, and the Gaza Strip.

[2] Painted by artist Filippo Minelli in 2007, for further details see Minelli (2019).

[3] The spatial and territorial connotations of cyberspace are themselves highly disputed conventions. On this topic, see Cohen (2007). Of course, countries regularly recur to offensive cyber operations targeting foreign infrastructures or users. When attributed, these are however commonly framed in terms of national security and preventive strategies.

[4] User mobility refers, in this article, to different forms of users' movement in cyberspace: access, handover, roaming, et cetera.

[5] On the concept of "territoriality rule" in cyberspace, please see Kostopoulos (2012).

[6] These include security contractors, commercial cybersecurity, service providers, as well the individual choices of users who, in this particular context, hold unique shares of responsibility.

[7] As theorized by Agamben in the *State of Exception* (2005).

[8] This territorial imaginary is also reinforced within interactive digital spaces, such as augmented-reality gaming (see Cristiano and Distretti 2017).

[9] This argument also provides the rationale for Israeli monitoring of parts of the Palestinian cyberspace that fall outside perceived territorial boundaries: Internet cafes in Jordan or Lebanon, but also pro-Palestinian international blogs and websites. In other words, the Israeli security apparatus operates on those spaces that are envisioned to be Palestinian regardless of their territorial configuration.

[10] These consist in taking control over a large number of unsuspecting computers (known in jargon as "zombies"). Joining these together into a robot network (the botnet), hackers use zombies to flood targeted websites with access requests until they collapse.