ROUTLEDGE COMPANIONS

Routledge Companion to Global Cyber-Security Strategy

Edited by Scott N. Romaniuk and Mary Manjikian

Palestine

Whose cyber security without cyber sovereignty?

Fabio Cristiano

in Romaniuk S. N. and Manjikian M. (2020, eds.) *Routledge Companion to Global Cyber-Security Strategy*, Basingstoke: Palgrave Macmillan.

A number of elements contributes to the absence of a centralized internet governance and coherent strategy for national cyber security across the Palestinian territory. With Israel in full control of network infrastructures, the Palestinian Authority (PA) and the Hamas administration retain limited sovereign functions with regards to cyberspace. Furthermore, the Palestinian governance of cyber security unavoidably echoes those territorial and political fractures that set apart the Palestinian Authority (PA) in the West Bank from Israeli-annexed East Jerusalem as well as from the Hamas administration in Gaza. These divergences are strikingly revealed in their dissimilar ways to engage with Israel: whereas the PA's approach takes the connotations of a cyber security cooperation, Hamas extensively recurs to its cyber-wings to launch attacks aimed at breaking the Israeli cyber-blockade. As a peculiar case of fragmented governance and limited sovereignty, Palestine provides a unique perspective to situate the concept of cyber sovereignty outside its traditional authoritarian narratives and to reveal its emancipatory potential.

Palestinian Authority:
the paradox of security without cooperation

National control over the infrastructural elements of cyberspace constitutes the primary condition for a country's ability to exercise its sovereignty online (Wu, 1997; Mueller, 2010; Jensen, 2015; Broeders, 2017). As an element of territorial sovereignty, countries ordinarily include 'their' national cyberspace in the compass of national security. Whereas cyber and digital sovereignty have been primarily engrained in those national narratives envisioning a tight control on cyberspace (Zeng et al., 2017; Budnitsky and Jia, 2018), these concepts assume an emancipatory connotation when applied to the context of Palestine.

In 1995, the Oslo II framework explicitly set forth the Palestinian Authority's (PA) right to nurture an independent ICT sector and autonomous national infrastructures: "the right to build and operate separate and independent communication systems and infrastructures including telecommunication networks, a television network and a radio network." (Annex III – Art. 36). In full violation of the peace agreement, however, Israel has until today precluded the possibility for Palestinians to fulfil their right to infrastructural autonomy (Abduaka, 2016). A 2016 World Bank report indicates that, besides retaining full control on the infrastructure, Israeli authorities regularly block the import of ICT equipment and technologies from abroad as well as their transit across the Palestinian territory (Rossotto, Decoster, Lewin, & Jebari, 2016). This tight control on infrastructural development also affects Palestinian mobile networks, a sector of rising

significance for cyber security. With Oslo I (1993) granting Israel jurisdiction over Area C – presently ca. 60 per cent of the West Bank[1] – Palestinian operators require multiple authorizations for importing and installing technologies in the area (AbuShanab, 2018). Indicating security concerns, the Israeli Civil Administration (ICA) regularly turns down Palestinian requests. Since 1967, Israeli authorities implement a building permit regime that hinders Palestinian construction and development in the West Bank and East Jerusalem. From 1993, and the institution of Area C, the bureaucratic procedures for Palestinians became even harder. Figures for 2016 (OCHA) indicate that the ICA rejected ca. 91 per cent of Palestinian building applications in Area C.

At the same time, and contrary to other network-based services – such as water and electricity – the architecture of cyberspace assigns control functions to the different nodes of the network, in a way that detaches sovereignty from infrastructural control (Mueller, 2019). Instead of a central unit governing the entire infrastructure, the national internet backbone comprises a conglomerate of main data routes that, connecting principal computer networks, sustains internet traffic and data mobility (van den Berg & Keymolen, 2017). This suggests that important sovereign functions are exercised through service provision: ISPs hold in fact a critical responsibility in securing the national cyberspace (also because they often own important data routes of the backbone), thus becoming crucial allies for national authorities (Yarden, 2005). In the current situation, however, Palestinian ISPs continue to be dependent to their Israeli homologues to provide internet connectivity across the PA-controlled areas of the West

Bank. Part of the PALTEL Group – a public sharing company founded in 1995 – the ISP Hadara controls the Palestinian market in its entirety, also thank to its controlled virtual operators.[2] Furthering the consequences of the Israeli occupation (cfr. UNCTAD, 2018), this *de facto* monopoly forces Palestinians to purchase an obsolete connection services at non-market prices. With these conditions, many prefer to purchase, illegally, internet services from Israeli operators. At the same time, Oslo I (1993) allows Israeli operators to supply internet connections and mobile services to illegal Jewish settlements in Area C. In East Jerusalem, Palestinian residents forcedly rely on Israeli internet service providers: putting "facts on the ground", Israeli annexation also bans Palestinian carriers and ISPs in their designated capital.

Lacking control over the infrastructure, and with very limited powers over service delivery, the PA holds a certain degree of regulatory prerogatives on information security, the primary element of interest for the most prominent narratives on cyber sovereignty (China and Russia). Operating through two focal aspects – content management/censorship and data traffic/access – the 2018 PA's cybercrime law[3] proposes to protect "national unity" and "social harmony" (Article 51) in its national cyberspace. Regarding the first aspect, it urges Palestinian ISPs – and hosting services – to take down those websites, blogs, and online contents that PA and its security agencies consider to be a threat to national security and values (cfr. Abdeen, 2018). With Palestinian contents already subjected to Israeli predictive policing and algorithmic scanning (Cristiano, 2019a), PA's surveillance further restricts freedoms for Palestinians. As second focal point, the PA's

legislation regulates access and data traffic for endpoints. Referring to security needs, the PA devoted various norms –as Article 31 – to outlaw connection via alternative routes, such as VPNs and the like (mesh networking, I2P, and more).[4] At the cost of violating liberties for users, banning these methods purports to constrain traffic along the national backbone. In the specific case, as this falls under Israeli control, the PA's ban on alternative connection methods ultimately forces Palestinian traffic on Israeli infrastructural networks. Peculiarly, the PA potentially punishes – with forced labor or jailtime – those users who recur to alternative connection methods to elude Israeli blocks and surveillance.

Concluding, despite its peculiarities, the PA case corroborates the argument of an accurate correspondence between national cyberspace and territorial sovereignty. The Israeli ban for Palestinian ISPs in East Jerusalem in fact extends the city's annexation to cyberspace. In the West Bank, Oslo's governance fragmentation and the Israeli occupation – with their complex regimes of access/mobility and regime of permits – are mirrored in PA's reduced sovereignty on its fragmented cyberspace. At the same time, the Palestinian case also suggests how sovereignty in cyberspace does not manifest solely as a function of infrastructural control, or service provision. Rather, PA's cyber security legislations reveal how implementing restrictive measures with regards to information security does not only violate digital rights, but ultimately gives away sovereignty functions and political authority on the altar of cyber security.

Hamas and the Gaza Strip: breaking the cyber-blockade

Palestinian internal fragmentation – both political and territorial – directly manifests in its divided national cyberspace. Following Hamas' 2006 victory in the Palestinian elections, Israel has imposed an illegal blockade on the Gaza Strip (Erakat, 2012). Severely limiting the mobility of goods and people, this measure further isolates the area from the rest of the Palestinian territory and results in the Strip's full reliance on Israeli infrastructures for the provision of basic services - such as electricity, water, and sewage treatment (The World Bank, 2018). Likewise, Israeli authorities and operators control Gaza's entire communication system, including wired and wireless internet services. With the extension of the blockade to bandwidth, spectrum, and frequencies allocation, Israeli authorities force the area into a state of technological obsoleteness (Fatafta, 2018).

In the Gaza Strip, internet governance shadows the one in place for the West Bank: relying on Israeli infrastructures, Palestinian ISPs deliver the service across the Hamas-controlled region (Tawil-Souri, 2012). Beyond this face-value equivalence, however, the overall service quality in the Strip endures the consequences of recent years' Israeli raids[5] on ICT infrastructures and of regular electric power cuts (Weinthal & Sowers, 2019). These, together with Israeli restrictions on Palestinian ISPs regarding infrastructural maintenance, often result in the area being disconnected from the internet (see Jalal, 2017).

In absence of regionally controlled infrastructural networks, and with extensive obstacles to regulate service delivery, the Hamas-led government ultimately retains marginal powers with regards to its national cyber security. In 2012, the party introduced a ban on the use of Israeli communication services (Ghraieb, 2012): with unavailable valid alternatives, this ban produced few results in gaining back control on traffic and market shares. Concerning information security, Hamas security agencies – through extensive monitoring – largely rely on policing users' data and contents to motivate arrests of political opponents and dissidents (AbuShanab, 2018). These same techniques are used for policing compliance to Islamic precepts: besides having enforced a ban on immoral websites[6] through ISPs, Hamas security forces regularly raid internet cafes to police users' online navigation. With little or no authority on infrastructures and service delivery, Hamas political strategy unfolds by tightening control on information security.

Besides implementing invasive security measures on its domestic information, Hamas' affiliated[7] cyber-wings routinely recur to disruptive operations to break the cyber blockade by targeting Israeli cyberspace, on both its military and civilian nodes. Hamas' offensive tactics include intrusive operations for gathering intelligence as well as disruptive ones. Whereas these intensify during Israeli raids on the Strip, they constitute an constant feature of regional warfare for the last ten years. Despite vastly asymmetric potentials in offensive and defensive cyber capabilities, these campaigns proved to constitute a great asset for Hamas' political strategy. They commonly rely on somewhat unsophisticated

coding but advanced social hacking techniques, crediting their success to highly designed baits. Targeting specifically military and governmental personnel, hackers recur to gaming, dating, and sport apps, or false links to leaked pictures and videos of IDF soldiers, to target users through highly tailored contents (IDF, 2017; ClearSky, 2018). In 2018, for instance, Hamas hackers implanted a spyware into an app mimicking the Red Alert, a service that alerts Israeli users in the event of imminent rocket attacks from Gaza (ClearSky, 2019; Cristiano 2019b).

On other occasions, Hamas hackers combine complex operations with well-developed social hacking techniques. One of Israel's basic cyber defense provision consists of blocking data coming from the Strip in order to prevent them reaching its network endpoints (AbuShanab, 2019). At these conditions, the success of Hamas' cyberattacks primarily depend on the ability of circumventing the Iron Dome-like barrier that extends the Israeli blockade to cyberspace. In 2015, Hamas 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 (TrendMicro, 2015). On one hand, the 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, the attack employed diverse bait contents for different targets, in line with social hacking's precept that envisions network vulnerability as the effect of users' behavior rather than of an

ineffective strategy of cyber security or defense (Bullée et al., 2018). In 2019, Hamas' offensive cyber warfare also lead to the first example of a real-time physical attack in response to a cyber-attack (cfr. Newman, 2019). With a tweet, the IDF in fact publicly announced that: "We thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we targeted a building where the Hamas cyber operatives work. HamasCyberHQ.exe has been removed."

Conclusion

Palestinian cyber security (and the lack thereof) reveals the complex relationship between territorial sovereignty and cyberspace. Limits to Palestinian autonomy in cyberspace do not only depend on lacking control over infrastructures, but also on the ways service delivery and the security of information are (not) governed by the Palestinian Authority in the West Bank and East Jerusalem, and Hamas in the Gaza Strip. In other words, claiming sovereignty over a national cyberspace requires more than controlling principal network routes and the infrastructure. As argued throughout this chapter, the complex territorial realities across the Palestinian territory put into question this equation. That is to say that cyber sovereignty decisively plays out as a function of information security, regardless of national control over the infrastructure.

The imposed restrictions to Palestine by the Israeli occupation appear to indeed create a continuity between national territory and cyberspace. The exceptionality of the Palestinian case, however,

illustrates how a country's sovereignty and its security in cyberspace appear to shape not only in terms of infrastructural control, but also as a result of dynamical political deeds. Above all, the PA cooperation on cyber security with Israeli security agencies – with the emblematic outsourcing of its organizational cyber security to the Israeli tech firm Check Point, Ltd. – accentuate the limits to its sovereignty in cyberspace. Pivotal in this cooperation, the 2018 PA cybercrime law hinders digital rights for its citizens while furthering Israeli control on Palestinian cyberspace. Adding on these, Palestinian users are subjected to two complementary regulatory regimes regarding the ways they can access the internet, protect their data, as well as sharing and managing their own contents.

Similarly, Israeli blockade on Gaza also manifests in the imposed siege on the Strip's cyberspace. In lieu of control on infrastructures and service delivery, Hamas authorities enforce their sovereignty and security through restrictive policies of information security. Along the same lines, the Islamic party's cyber-operations – through social hacking and expedients for bypassing territorial blocks – somewhat disown the argument that the national boundaries of cyberspace can be identified through its physical infrastructures or territorial identifiers (e.g., IPs, domain names). In other words, sovereignty is configured as a dynamic and political feature of cyberspace.

In terms of cyber security, accounting for this dynamicity requires envisioning cyberspace as more than a nationally controlled infrastructural system. In this light, the Palestinian case evokes the

importance of including service provision and information security into the compass of a long-sighted national strategy.

References

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

Abduaka, M. (2016). "The Telecommunication and IT Sector in Palestine," *TWIP*, *223*(1): 17–23.

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

AbuShanab, A. (2019). "Hashtag Palestine 2018: An Overview of Digital Rights Abuses of Palestinians," *7amleh – The Arab Center for the Advancement of Social Media*.

Broeders, D. (2017). Aligning the international protection of 'the public core of the internet' with state sovereignty and national security. *Journal of Cyber Policy*, 2(3), 366-376.

Budnitsky, S., & Jia, L. (2018). Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance. *European Journal of Cultural Studies*, 21(5), 594-613.

Bullée, J., Montoya, L., Pieters, W., Junger, M. & Hartel, P. (2018). "On the Anatomy of Social Engineering attacks—A Literature-based Dissection of Successful Attacks," *Journal of Investigative Psychology and Offender Profiling*, *15*(1): 20–45.

ClearSky. (2018). "Infrastructure and Samples of Hamas' Android Malware Targeting Israeli Soldiers". Cambridge: Clearsky Security, Ltd.

ClearSky. (2019). *Year of the Dragon: 2018 Cyber Events Summary Report*. Cambridge: Clearsky Security, Ltd.

Cristiano, F. (2019a). "Internet Access as Human Right: A Dystopian Critique from the Occupied Palestinian Territory," in G. Blouin-Genest, M.-C. Doran & S. Paquerot (eds.), *Human Rights as Battlefields* (pp. 178–201). Basingstoke: Palgrave Macmillan.

Cristiano, F. (2019b). "Deterritorializing Cyber Security and Warfare in Palestine: Hackers, Sovereignty, and the National Cyberspace as Normative". *CyberOrient* 13(1), pp. 28-42.

Erakat, N. (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*(37): 40–83.

Fatafta, M. (2018). "Mapping of Digital Rights Violations and Threats". Published by 7amleh - The Arab Centre for Social Media Advancement and The Association for Progressive Communications (APC).

Ghraieb, O. (2012, September 3). "New Internet Censorship Rules Take Effect in Gaza," *The Jerusalem Post*.

IDF. (2019, May 5). "CLEARED FOR RELEASE: We thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we targeted a building where the Hamas cyber operatives work. HamasCyberHQ.exe has been removed". Retrieved from: https://twitter.com/IDF/status/1125066395010699264

IDF. (2017, April 5). "Hamas Uses Fake Facebook Profiles to Target Israeli Soldiers". *IDF's official website*.

Jalal, A. (2017, July 9). "How Gazans are Dealing with Internet Crisis," *Al Monitor*.

Jensen, E. T. (2015). Cyber sovereignty: The way ahead. *Tex. Int'l LJ*, 50, 275.

Mueller, M. L. (2010). *Networks and states: The global politics of Internet governance*. MIT press.

Mueller, M. L. (2019). "Against Sovereignty in Cyberspace". *International Studies Review*.

Newman, L. H. (2019). "What Israel's Strike on Hamas Hackers Means For Cyberwar", *Wired,* June 5.

OCHA. (2017). *oPt Fragmented Lives: Humanitarian Overview 2016*. East Jerusalem: United Nations Office for the Coordination of Humanitarian Affairs occupied Palestinian territory.

Rossotto, C., Decoster, X. S., Lewin, A. & Jebari, I. (2016). *The Telecommunication Sector in the Palestinian Territories: A Missed Opportunity for Economic Development*. Washington, DC: The World Bank Group.

Tawil-Souri, H. (2012). "Digital Occupation: Gaza's High-Tech Enclosure," *Journal of Palestine Studies*, *41*(2): 27–43.

TrendMicro. (2015). "Operation Arid Viper: Bypassing the Iron Dome." TrendMicro Research Team.

United Nations Conference on Trade and Development. (2018). "Report on UNCTAD's Assistance to the Palestinian People: Developments in the Economy of the Occupied Palestinian Territory," United Natoins, Geneva, Switzerland.

van den Berg, B. & Keymolen, E. (2017). "Regulating Security on the Internet: Control versus Trust," *International Review of Law, Computers & Technology*, *31*(2): 188–205.

Weinthal, E. & Sowers, J. (2019). "Targeting Infrastructure and Livelihoods in the West Bank and Gaza," *International Affairs*, *95*(2): 319–340.

The World Bank. (2018). *Economic Monitoring Report to the Ad Hoc Liaison Committee*. Washington, DC: The World Bank Group.

Wu, T. S. (1997). "Cyberspace Sovereignty: The Internet and the International System," *Harvard Journal of Law & Technology*, *10*(3): 647–666.

Yarden, J. (2005, December 16). "Should ISPs Be Accountable for Overall Internet Security?" *TechRepublic*.

Zeng, J., Stevens, T., & Chen, Y. (2017). China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty". *Politics & Policy*, 45(3), 432-464.

[1] Estimations regarding the extension of Area C vary. This variation depends on whether percentage includes East Jerusalem, the so-called "no man's land," and the Palestinian share of the Dead Sea. The extension of Area C underwent different changes throughout recent history. During the first phase (1993–1995), Area C constituted a total of 72–74 per cent of the West Bank. In accordance with the Wye River Memorandum, an additional 13 per cent should have been incorporated in Area B through Israeli withdrawal from Area C – thus reducing its area to a total of 61 per cent. In contravention of the memorandum, Israel only withdrew from a total of 2 per cent, which eventually re-occupied in 2012. As a result, as of 2013 the common figure estimates Area C to constitute the 63 per cent of the West Bank.

[2] Virtual mobile operators (VMOs) resell internet services without having ownership of the infrastructures. Their activities and degree of independence are contingent on contracts and partnerships they stipulate with ISPs. VMOs commonly develop their own branding, marketing, sales and invoicing systems, as well as customer support.

[3] The full English translation of the Presidential Decree No. 16 is available at: https://goo.gl/Dj1t1Q

[4] Besides VPNs, other methods exist to re-route one's connection outside main national data routes. Commonly used by large companies and institutions, proxy

servers allow to encrypt data through connecting one's device, a single endpoint, with a remote small network (or a single endpoint) that obtains content on device's behalf. Using end-to-end encryption, the invisible internet protocol (I2P) enables anonymous connection through a global network of over 55k volunteer computers. Based on a similar cooperative structure, a particular type of local network topology – referred to as meshnetworking – allocates to each network node the possibility to connect directly and dynamically.

[5] Since 2008, Israeli military conducted three major assaults on Gaza that inflicted enormous damages to ICT infrastructures.

[6] Part of a broader strategy to forcefully "re-establish morality and protect Gaza's social fabric," in 2008 Hamas had already signed an agreement with PALTEL for applying access filters on websites displaying explicit contents. In 2012, the Islamic group extended this measure to all ten ISPs operating in the Strip.

[7] Because of the illicit nature of their activities, unless self-claimed, the relationship between Gaza hacker groups and Hamas remains unclear. The ties between cyber-armies, proxies, hacker groups with states often tend to be ambiguous. Whereas some national armies officially set up cyber-units (as, for instance, in the case of the cyber-wing of the IDF), others do so without officially disclosing the existing connection between the state and the cyber-army. Intuitively, this allows countries to elude state attribution with regards to illegal cyber-operations.