Article

Digital Surveillance/Militant Resistance: Categorizing the "Proto-state Hacker"

Television & New Media
1–16

DOI: 10.1177/1527476418793509
journals.sagepub.com/home/tvn
SAGE

Erik Skare[1]

Abstract

Rapid developments in digital infrastructure have made all-encompassing surveillance all too possible. However, the same infrastructure has simultaneously enabled the use of new possibility spaces that react to, shape, and resist these structures of control and surveillance. The Israel/Palestine conflict is no different, and Palestinian Islamic Jihad (PIJ) has created an electronic unit with hackers to circumvent and resist the Israeli matrix of control and its surveillance. I argue that out of this dialectical relationship in Palestine, between new possibility spaces of resistance and structures of control, new phenomena arise in the gray area between the nation state hacker and the hacktivist as PIJ emulates the features of a modern state army. To understand the nature of its electronic unit, one must take this dialectic into account by introducing the category, "proto-state hacker."

Keywords

Palestine, Israel, Palestinian Islamic Jihad, hacking, proto-state hacker, digital resistance

Introduction

Rapid developments in the cyber-infrastructure have made all-encompassing surveillance all too possible, and today we know that every keystroke, each mouse click, every purchase, tweet, scan, Google search—in short, everything that we do in the digital age can be recorded, stored, and monitored (Harcourt 2015, 1). Indeed, the small, numerous, pieces of information that we leave behind do not tell much alone, yet, the sum of all those parts do give a worryingly descriptive picture, not just of what we do but also of who we are as human beings. As Morozov notes, "in the past, states

[1]University of Oslo, Norway

Corresponding Author:
Erik Skare, Doctoral Research Fellow, Department of Culture Studies and Oriental Languages, University of Oslo, PB1010, Blindern, Oslo 0135, Norway.
Email: erik.skare@ikos.uio.no

used to torture to get this kind of data; I mean, now all you have to do is get on Facebook" (The RSA 2011).

These structures of surveillance are not limited to Europe and North America, but are also a fundamental part of the Israeli occupation of the Palestinian territories, a multifaceted structure that Halper (2015) terms the "matrix of control." This Israeli matrix of control is manifested not only in physical obstacles such as the Separation Wall in the West Bank or numerous checkpoints and settlements but also by a vast digital-military complex with an extensive surveillance of the Palestinian population. However, simultaneously as the developing cyber-infrastructure has created new and vast opportunities for control and surveillance, the same structures have also created new opportunities to resist these developments by translating acts of direct action and civil disobedience into virtuality (Jordan and Taylor 2004), onion routing and IP address spoofing, or social mobilization and activism, to mention some. With the Palestinian population living under the Israeli matrix of control, we see that both Palestinian activists and militant factions employ and benefit from the possibilities enabled by technology while the Israeli occupation controlling them is being saturated and more all-encompassing.

This development also includes PIJ, a Palestinian Islamist militant movement that emerged in the Gaza Strip in 1981, and which emphasizes that only armed struggle can liberate the occupied Palestinian territories. As PIJ is divided into a political and a military wing, the latter has developed an electronic unit for circumventing Israeli structures of surveillance and to carry out hacking operations.

This article is based on an interview and discussions with the main representative of PIJ in the West Bank, carried out as a part of extensive fieldwork in the West Bank from September to December 2014, and an analysis of its magazine *Muqatil al-Saraya* (*The Brigades' Fighter*), publicly available on its armed wing's website.[1] I show that the dialectical relationship between the opportunities for control and resistance creates a new phenomenon unaccounted for in the current hacker taxonomies. As the electronic unit of PIJ employs both offensive hacking campaigns and defensive measures, the military wing in which the electronic unit resides has consequently begun to emulate the features of a modern state army. Although the electronic unit hacks for political and social causes, it differs from the hacktivist by virtue of its organizational subordination in a militant organization. Although the electronic unit is tasked with both surveillance and countersurveillance, it lacks the capabilities and means of modern nation state hackers. Thus, the electronic unit is forced into a gray area between the two, making it necessary to introduce a new hacker category, "the proto-state hacker."

This article consists of four parts. First, I assess the pervasive surveillance enabled by the new cyber-infrastructure, which enforces and saturates structures of control. I argue that, simultaneously, the very same infrastructure creates new opportunities to resist these structures. Second, I assess the Israeli matrix of control and how PIJ has adapted to (and maneuvered within) this framework by introducing an electronic unit resisting its structures. Third, I argue that a new phenomenon arises from its dialectics, which is unaccounted for in the current hacker taxonomy, and I will here introduce a

new category, "the proto-state hacker." Last, I conclude my findings and propose subjects in need for further research.

Circumventing Structures of Control and Surveillance

Surveillance is an essential mechanism of power, which emanated long before the emergence of the Internet in its modern form, and, as analyzed by Foucault, surveillance was one of the key features of the disciplinary society in the eighteenth and nineteenth centuries. As the judicial system was adjusted to a mechanism of control, an organ of generalized and constant oversight emerged, through which "everything must be observed, seen, transmitted." With the integration of oversight and control into a centralized state apparatus, Foucault asserts that the nineteenth century founded "the age of panopticism" (Foucault 1994, 32–35).

Today, the disciplinary society of Foucault seems to be of distant past in terms of sophistication and extent. However, as a mechanism of control, its function not merely persists, but expands as, "under conditions of surveillance capitalism, those who hold, manage and control the personal data of digital citizens are offered unprecedented insights into our lives, minds and bodies" (Hintz et al. 2017, 732). This was unmistakably made clear when the Guardian published the revelations of the whistle-blower Edward Snowden, which exposed the indiscriminate, and widespread, monitoring of everyday communication by the intelligence agencies National Security Agency (NSA) and Government Communications Headquarters (GCHQ) (Dencik and Cable 2017, 763). As Hintz and Dencik (2016, 2) note, the leaks "[transformed] our understanding of how our online activities are monitored," and according to Bauman et al. (2014), the scale, reach, and technical sophistication of the practices revealed came as a surprise even to seasoned observers.

The revelation of these surveillance programs underscored the extent to which contemporary governance is increasingly based on "the ability to monitor, track and potentially predict the behaviour of entire populations" (Dencik et al. 2016, 2). According to Karatzogianni and Gak (2015, 132), the leaks implied a logic for contemporary securitizing governmental power to "take every digital communicative act to be pernicious unless proven innocuous." Indeed, a central concern for Snowden was the extent to which mass surveillance stifles the possibilities of challenging institutions of power and it did prove to have disciplining effects as reports of self-censorship emerged in the wake of the leaks (Dencik et al. 2016, 2).

What is distinctively new from the disciplinary societies of the eighteenth and nineteenth centuries, however, is not merely the amount of data traced and stored, or its production, but also the fact that today we willingly provide it through the everyday technologies and media that we use. As van der Velden (2015, 186) notes, data leakage (feeding off already circulating data) is one of the basic methods of collecting data for the NSA. Lyon (2014, 11) concludes that, " . . . those revelations on Big Data practices, also lay bare in ways that were known only hazily before just how far security and intelligence agencies depend on data obtained from the commercial realm."

Correspondingly, the symbiosis between intelligence and the commercial realm is, by Harcourt (2015, 215), described as,

> a tenticular amalgam of public and private institutions that includes signal intelligence agencies, Netflix, Amazon, Microsoft, Google, eBay, Facebook, Samsung, Target, and others . . . all tied up in knots of statelike power. Economy, society, and private life melt into a giant data market for everyone to trade, mine, analyze, and target.

I do not intend, however, to draw a dystopian picture of society and its developments. Instead, my argument is twofold. First, as already noted, the development of the cyber-infrastructure has made surveillance possible on a scale unseen due, partly, to the creation, collection, and analysis of Big Data within the framework of contemporary capitalism. However, second, the very same developments have also created new opportunities to resist and circumvent the same structures of control and surveillance.

After the Snowden leaks, for example, we have witnessed a renewed focus on and an interest in privacy-enhancing tools such as the Tor browser, the Pretty Good Privacy (PGP) e-mail encryption system and encrypted messaging software such as Signal (Dencik et al. 2016, 4). Today, protesters can coordinate on the fly through social media, while in the past, the police had a largely one-sided advantage with radios, helicopters, and specialized training (Tufekci 2014, 11). Furthermore, WikiLeaks illustrates how information and communication technology has been employed innovatively for social change and bypassing information restriction (Hintz 2012, 88), and Karatzogianni and Robinson (2014, 2705) even describe WikiLeaks as a digital Prometheus, the trickster who "stole the fire," with its attempt to break government and media corporate infrastructure. As WikiLeaks describes itself as "the first intelligence agency of the people," the whistle-blowing platform turned the Foucauldian logic of surveillance as the knowledge of whether an individual is "behaving as he should, in accordance with the rule or not" on its head (Fuchs 2011, 2). That is, with the leaks, the state no longer exercised a monopoly of monitoring behavior, but suddenly found itself monitored by an external agent exercising discipline. As phrased by Karatzogianni (2017, 11), intelligence agencies were put in "an impossible position of forced transparency."

This dual nature of the Internet—enabling mass surveillance, anonymity, and control—is then partly because of the values built into its layers, in which one layer does not necessarily affect the values of other layers. As Zajácz (2013, 493) notes, "WikiLeak's focus on strong, cryptographic anonymity as a norm for online participation amplifies the values embedded in the network's control software, while Facebook's requirement of identification negates those values via corporate policy."

Two things are, however, important to emphasize at this point. First, the structures of control and the resistance to it are not binaries external to each other but instead are in constant interaction and contact through which both influence and shape each other. For example, while social platforms ease political mobilization from below, governments learn how to respond to more open public spheres, for example, by

flooding the space with "trolls" to make digital spaces difficult to navigate (Tufekci 2014, 6). Although they also provide opportunities for more rapid mobilization and organization of protests, in the long term, protests can also be made more vulnerable (Tufekci 2017). Although the Internet eases interactivity between people and political deliberation, "digital participation is reflexive in the sense that it generates information about itself," which can be mined and controlled (Andrejevic 2016, 188). Last, while the Internet enables Israeli and Palestinian human rights organizations to document the occupation, it also enables the Israeli army to produce "an exquisite and highly sanitized visual archive of soldiering . . . in which war is simultaneously heroized and aestheticized while disassociated from resultant violence" (Kuntsman and Stein 2015, 2).

Second, the current struggle between structures of control and the attempts to circumvent them constitute a continuation of past struggles lost and won. As Coleman and Golub describe, when Phil Zimmerman developed a method for encryption on personal computers in 1991, today known as Pretty Good Privacy (PGP), it was not merely a robust piece of technology, but an act of civil disobedience that flew in the face of intellectual property and national security laws. Although Zimmerman believed in privacy for everyone (and not just for intelligence agencies and large corporations), the American state perceived the technology as a violation of disclosure and a transfer of munition (Coleman and Golub 2008, 259). The act of Zimmerman was in other words a struggle for what the Internet was, what it should be, and for whom it should be. Indeed, there is a Zimmermanian echo in the words of Rogaway when after the Snowden leaks the latter stated, "[e]ncryption rearranges power: It configures who can do what, from what. This makes cryptography an inherently *political* tool, and it confers on the field an intrinsically *moral* dimension" (Rogaway 2015, 1).

Corresponding to this particular ethos of the free Internet, one of the early acts of hacktivism—defined as "the marriage of political activism and computer hacking" (Samuel 2004, 102)—occurred when the first commercial e-mail was sent to all Usenet users April 1994 and the transmitter was inundated by so many angry e-mails in reply that the advertiser's inbox shut down. As McChesney (2013, 97) points out, the notion among the Usenet users then—which led to this digital form of protest—was that commercialism and Internet democracy could not, and should not, merge. Hacktivism has since then developed extensively, both the means employed and the actors engaging in it, and it is outside the scope of this article to delve into all of its particularities and developments. Yet, it is possible to identify shared perception of the phenomenon in academic research. Whereas Samuel (2004, 102) states that "hacktivism combines the transgressive politics of civil disobedience with the technologies and technique of computer hackers," Coleman (2017, 99) notes that both WikiLeaks and hacktivist collectives such as Anonymous "challenge status quo channels of debate and official, legally sanctioned domains of politics . . . [and] demonstrate a more forthright, hands-on engagement with politics." Correspondingly, "we should approach the phenomenon of hacktivism as a new kind of protest that is historically conditioned: protests during the digitalization of political pressure" (Skare 2016, 10). Thus, hacktivism is a

distinct form of political direct protest enabled by the opportunities of the new cyber-infrastructure to engage digitally in political struggles through which,

> Hacktivism attempts to translate the principles of direct action into virtuality. The sit-in or blockade that occurs in the streets and aims to cause a meeting to fail, can be matched by a blockade of online messages, which aims to make computer support for the meeting to fail. (Jordan and Taylor 2004, 69)

Although this outline cannot heed justice to all of the various forms of resistance against the structures of control and surveillance due to the scope of this article, my point is nevertheless that out of the new possibilities that the developing cyber-infrastructure provides, a continuous process of surveillance and resistance develops within the same confines. This dialectic is certainly summarized in the words of Foucault (1990, 95), "[w]here there is power, there is resistance, and yet, or rather consequently, this resistance is never in a position of exteriority in relation to power." If surveillance ensures power, it also produces the resistance to it. It is in this continuous process of surveillance, control, and resistance—with its emerging and inherent contradictions—that I argue the phenomenon, the "proto-state hacker," arises.

Adapting to the Structures of Control: PIJ and Its Electronic Unit

The Israel/Palestine conflict is not only an exemplifying case because it illustrates the interplay between structures of surveillance and control, and the resistance to it, but also because the Israeli technological-military occupation saturates and strengthens the expressions of this dialectic. Indeed, today, through the Israeli specialization in encoding systems, sensor and signal processing, software, passive and active electronic countermeasures, image processing, and display and surveillance systems, "[t]he Occupied Palestinian Territory has been transformed into probably the most monitored, controlled and militarized place on earth" (Halper 2015, 143).

The technological-digital features of the Israeli control structures are only in addition to their physical manifestations with the settlements, roadblocks and checkpoints, the Separation Wall, the blockade of Gaza, and the fragmentation of the West Bank. As Weizman (2007, 15) argues, these physical manifestations are an important feature of the structures of control as

> These massive [Israeli] infrastructural systems, drawing provisional borders through sovereign three-dimensional spaces, are the physical infrastructure of a unique type of political space, one desperately struggling to separate the inseparable, by attempting to multiply a single territorial reality and create two insular national geographies that occupy the same space.

The analysis of Weizman and Halper's concept of the occupation as a "matrix of control" is then exemplified in the concept of "technological politics," which Dafoe (2015, 1053) describes as the ideas inscribed into technologies, which then influence

others—in this case the Palestinians. Referring to Lay (1992), Dafoe (2015, 1053) uses the examples of fences, speed bumps, bulletproof glass, surveillance technology, encryption algorithms, and the broad linear Parisian boulevards that facilitated the suppression of riots, which are, as shown, always existing features of (the lack of) life in the Palestinian territories. In that sense, the Israeli matrix of control in its entirety—from the physical to the technological manifestations—epitomizes Pötzsch's (2015, 111) concept of "iBorder," "a sociotechnological apparatus that employs techniques of biometric and algorithmic bordering to validate, establish, and indeed, produce, identities and patterns of life." Conversely, Deleuze's (1992, 7) concept of "societies of control" as an extension of Foucault's disciplinary society is descriptive of this digital-material complex with checkpoints and walls as he pictures spaces in which one can leave one's apartment, street or neighborhood with an electronic card, but which can just as easily be rejected on a given day or between certain hours.

The manner in which this matrix of control, the iBorder, or the society of control is produced, and maintained, has certainly been subject to change in accordance with the introduction of new technology and the technological politics inscribed in it. For example, the Israeli withdrawal from the Gaza Strip, 2005, was largely grounded in the belief in (and support of) replacing material control mechanisms such as roadblocks and soldiers on the ground with an "aerially enforced occupation" with a "vacuum cleaner" approach to intelligence gathering and surveillance through the high-tech drones always floating above the Strip (Weizman 2007, 239–40).

Palestinians have felt the effects of this digital-material matrix of control in general and Israeli surveillance of social media in particular, and several have been arrested for "incitement" on Facebook (Kane 2016). The surveillance of Palestinians on social media has also shown to lead to bizarre situations as a Palestinian was arrested after writing "good morning" in Arabic, which Israeli police mistakenly had translated to "attack them" (Smith 2017). This is not limited to the Israeli occupation, of course, but also to the Palestinian Authority who arrested Ayman Mahareeq after the latter published the following status update on Facebook, "May the rule of the Palestinian Authority collapse" (Harris 2015).

The effects of the developing cyber-infrastructure has, however, not been one-sided, and although the Israeli structures of control have become more saturated, also the Palestinians have exploited the possibilities enabled by the Internet. The last decade, for example, several Palestinian hacktivist teams such as Gaza Hacker Team have emerged with hundreds of attacks against the Israeli cyber-infrastructure. Necessarily, the tactics, scopes, and frames of this part of the Palestinian resistance is affected and shaped by the Israeli structures of control. Whereas Coleman and Golub (2008, 257) identified three moral genres of hacking, which are all in the traditions of liberalism, Palestinian hacktivist teams appropriate religious and political signifiers and symbolism ranging from traditional Palestinian secular-nationalism to conservative militant Salafism (Skare 2016). Second, as noted, while a number of hacktivist teams in the West employ digital direct action to effectuate change, they largely do so in negotiation with power on issues such as human rights, free speech, and Internet freedom, to mention just some. The Palestinian hacktivists, on the contrary, do not

engage in any negotiation with power, but seek instead its liquidation because the dismantling of the Israeli occupation is the very precondition for achieving liberation (Skare 2016). Indeed, as described above, Coleman notes that hacktivists challenge (democratic) status quo channels of debate in addition to official, legally sanctioned domains of politics; yet, these do not exist for ordinary Palestinians in terms of dismantling the structures of control imposed on them from the outside.

The hacking of the Israeli cyber-infrastructure extends to the Palestinian armed factions as well. During the Israeli bombing of the Gaza Strip in November 2012, for instance, PIJ hacked into a government website, obtained 5,000 top Israeli military and government officials e-mail accounts, and sent them messages stating that "Gaza will be the graveyard of your soldiers and Tel Aviv will be a ball of fire," written in Hebrew (Skare 2016, 117). Furthermore, in March 2016, a member of PIJ was convicted of hacking the video feed of Israeli drones hovering over the Gaza Strip (Bob 2017), thus turning the inspecting eye on them against its beholder.

Yet, much indicates that the hacking campaigns constitute an exception to the cyber-activities of PIJ. The main representative of PIJ in the West Bank, for example, stated in an interview that the electronic unit was founded in 1999 with the sole purpose of keeping pace with the technological developments of the Israeli structures of control. Furthermore, he emphasized that the main goals of its electronic unit are not primarily hacking Israel, but instead, (1) to prevent electronic attacks from Israel; (2) to prevent espionage and surveillance; and (3) to spread the Palestinian cause to the rest of the world and international media (PIJ main representative West Bank, interview with author, November 16, 2014). This focus on defensive measures corresponds to the approach espoused in PIJ's magazine, *Muqatil al-Saraya* (The Brigades' Fighter), through which it emphasizes the defensive needs and dangers of technology. For instance, the question posed in all articles concerning technology is the following: How can one protect oneself from Israeli surveillance?

The defensive focus on technology proposed by both the main representative of PIJ in interviews, and in its magazine, *Muqatil al-Saraya*, must be analyzed within the Israeli structures of control, and further within the confines of the electronic unit's development with the eruption of the Second Intifada (2000–2004). For example, the State of Israel has employed the policy of assassinations since before its foundation in 1948. Yet, from initially constituting an exceptional emergency method, "[w]hat was new [with the policy of assassinations during the Second Intifada] was the scale of the effort—never have so many [Palestinian] militants been killed in such a short span of time" (David 2002, 117). Today, "[assassination] has become the Air Force's most common form of attack" (Weizman 2007, 238), and from 2000 until 2004, approximately two hundred assassinations, either acknowledged by Israel or beyond dispute, were carried out, although the numbers are far greater with weekly incidents of Palestinians being killed during raids (Hroub 2004, 28). Indeed, the Israeli policy of assassinations depends greatly on the structures of surveillance, of which Palestinian militants have felt the effects. Hamza Abu al-Haija, for example, one of the leaders of Hamas military wing, the Izz al-Din al-Qassam Brigades, was assassinated by the Israeli army after it discovered his location through his personal Facebook account

(Abu Amer 2015). I do not assert, however, that there is a direct causality between the assassinations and the manifestation of defensive measures in PIJ's electronic unit; I instead describe the context in which it developed and operated. That is, shortly after the electronic unit of PIJ was established in 1999, the conflict escalated sharply with the eruption of the Second Intifada, with a corresponding surge in the number of Israeli assassinations. This was coupled with the advancing capabilities of surveillance in the hands of the Israelis.

The defensive focus of the electronic unit, to prevent Israeli surveillance and espionage, does then to a certain extent, and within a differing context, illustrate the development described above in this article when currents, groups, and individuals on the ground adapt to and circumvent surveillance and structures of control by re-appropriating the very same tools and methods used against them. If activists and ordinary citizens rearrange power through encryption, so does PIJ through its electronic unit. Just as WikiLeaks turns the Foucauldian logic of surveillance on its head by using it against structures of power, so does the electronic unit hack and exploit the tools of surveillance used against them, such as drones. Several statements of PIJ embody this dual nature of the new structures of control and surveillance, and the opportunities provided by the same cyber-infrastructure. For example, on one hand, PIJ writes, "Our war is with the most dangerous intelligence service in the world, which is the most modern and technical." Yet, it continues by emphasizing that "[e]lectronic warfare is no longer confined to the Zionist army, and the Palestinian resistance, and its vanguard, the Jerusalem Brigade, in particular, has made some [electronic] achievements" (Muqatil al-Saraya 2013, 12).

It is important to note that this duality of the cyber-infrastructure is neither particular nor new, as Palestinians in the physical realm, fenced in behind the walls of the occupation, dig tunnels underneath to circumvent, and cancel the structures of control. The relationship between power and the subjugated, between the gatekeeper and controlled, influences then both actors involved in the exchange through which we see their continuous adaption to each other in a series of reciprocal actions in which the subject and object at hand is reproduced. It is from this reproduction of object and subject a new phenomenon emerges that has not been taken into account in the current hacker taxonomies, the "proto-state hacker."[2]

Making the Case for the Proto-state Hacker

In fact, assessing the hacker taxonomies of Rogers (2006), Hald and Pedersen (2012), and Seebruck (2015), there are no categories that fit the electronic unit of PIJ, and only two of them resemble its features: the hacktivist and the nation state hacker. First, the electronic unit of PIJ resembles the hacktivist insofar as it hacks to obtain political change (the criteria of the motivation). However, as shown, hacktivism is of a distinct activist nature, which does not correspond to the military nature of PIJ's electronic unit. Indeed, the organizational profile of the electronic unit does not fit as the hacktivist teams are often described as collectives, while the electronic unit is a part of a military wing with its own set of rules, organizational structures, and hierarchy. To equal the

hacktivist with the electronic unit would either be to equate a part of PIJ's military wing to some sort of activism, or conversely to elevate the hacktivist to a military level. None of these options are satisfactory in terms of analysis and conceptual meaning.

If one then wishes to balance between the hacking operations that PIJ's electronic unit has carried out in the past, referenced above, and its primarily defensive role emphasized by PIJ's representative in interviews, one could then attempt to see if the unit fits into the category of the nation state hacker. This would be meaningful insofar as the nation state hacker embodies both defensive and offensive means and tasks as a part of a military infrastructure with a high level of secrecy. Illustratively, the main representative of PIJ noted the importance of avoiding publicity, "We work in silence and in calm in order to achieve our goals and defeat the occupation" (PIJ main representative West Bank, interview with author, November 16, 2014).

Yet, as the current taxonomies focus so heavily on skills (in addition to motivation), this would ignore the fact that (advanced) nation state hackers "have access to more funds, better equipment, and more thorough intelligence than any other groups of attackers. Their resources are vast" (Hald and Pedersen 2012, 85). There is nothing that indicates that the electronic unit of PIJ has the resources to be considered as equal to technologically advanced nation states such as the United States, China, Israel, or Russia, which are most likely some of the states implicitly referred to in the previous taxonomies, contrary to less developed states such as Afghanistan and Somalia.

This implies that we cannot limit the criteria in the hacker taxonomies to that of skills and motivations, as the aforementioned hacker taxonomies do. Indeed, these two classifiers are at the onset not particularly robust as a hacker group with severely limited skills can create great havoc if they have access to substantial resources—such as a botnet (a number of Internet-connected devices, which can be used to perform tasks such as distributed denial-of-service attacks) consisting of millions of (hypothetical) computers. Israel itself illustrates the skill/resources dilemma because highly developed high-tech states become increasingly exposed corresponding to their dependence on information technology, and Israeli army officials have stated that a cyber-attack on Israeli critical infrastructure could be more harmful than a missile attack (Ahronheim 2017). Correspondingly, despite (or perhaps because of) the limited set of skills required, Hamas was able to create a honey trap in 2017 through the creation of a number of fake Facebook profiles, adding Israeli soldiers as friends and engaging in conversation with them to obtain information on Israeli military plans and deployments (Ackerman and Khrennikov 2017).

To summarize, PIJ is an example of a military movement that adapts to structures of control and surveillance, through which we see the emergence of hackers (simultaneously defensive as offensive) within the structures of and subordinated to the decision-making in hierarchical organizations. It is precisely because the electronic units cannot be considered an autonomous actor outside of the organizational framework that the assessment of its motivations is insufficient. Instead, it is subject to and governed by the movement overall, by a hierarchical structure with a set of rules, principles, and guidelines to follow. It has a secondary function to the movement's main task, armed action, and it is the latter that the former has to support, assist,

and facilitate as PIJ attempts to adapt to the structures of control. By virtue of the organizational subordination of the electronic unit under PIJ's military wing, it does much more resemble that of, and emulates the features of a modern state army with an electronic unit that is employed for countersurveillance, espionage, and offensive cyber warfare. As the organizational subordination distinguishes the electronic unit from the hacktivist, it is by far inferior to the nation state hacker, and it thus falls in a gray area between the two—between motivations and resources.

I thus propose the introduction of the category "proto-state hacker" to describe the electronic unit of PIJ, as its tasks so closely resemble those of the nation state hacker, while being far from the latter in resources, skills, and capabilities. It is important to emphasize that this new phenomenon, the "proto-state hacker," arising as PIJ adapts to the Israeli structures of control with the emulation of a modern state army, is not a teleological feature inscribed in the dialectic between surveillance and resistance, but instead an example of when introduced technologies have unintended consequences (Dafoe 2015, 1054). This particular unintended consequence of the Israeli structures of control and PIJ's adaptations to it is then strikingly similar to the emergence of the hacktivist, described above, who was created and shaped in the nodal point between the Internet's democratizing potential and its commercialization. Yet, the "proto-state hacker" emerges within another context, and the category captures the long-existing trend of a militarization of the Internet. Not simply because governments and states employ the Internet as yet another field of battle, but because also armed clandestine movements that strive for statehood employ the very same means as they adapt to the behavior of the states they fight. As PIJ has grown and adapted in accordance with the overall technological development, seeing the necessity of the cyber-infrastructure for its armed activities, it employs the electronic unit to assist the facilitation and ease of that very armed activity within the Israeli matrix of control. Yet, while doing so, it is incapable of matching the resources and capabilities of the states that it emulates.

Conclusion

We have seen that the developing cyber-infrastructure has saturated and strengthened all-encompassing surveillance. Yet, the very same infrastructure has also provided the tools to circumvent and resist it. The Israel/Palestine conflict is no different, and the dialectical relationship between Israeli control and Palestinian resistance to it has produced the unintended consequence of the "proto-state hacker" through emulating the features of a modern state army.

The category "proto-state hacker" provides meaning to an inherently *social* configuration that so far is insufficiently analyzed. This emphasis is important because the categories that we apply to a wide range of actors have qualitative effects on how we approach groups and actions online, as the very categories embody both hidden and apparent connotations. If one limits oneself to false definitions and categories, exoticize online actors and actions, or employ moral binaries, then we will also lose our ability to fully understand and appreciate the significance of these agents as social political actors.

Indeed, the category "proto-state hacker" is an enduring one as it can be applied to any armed conflict in which a nonstate party adapts to structures of control by exploiting the new opportunities for surveillance, countersurveillance, and hacking campaigns, thus emulating the features of a modern state army without equaling the latter in capabilities and resources. As we are witnessing an increasing militarization of the Internet, it is likely that this will become more common in the future. The Islamic State (IS) is perhaps the case most closely resembling the "proto-state hacker" of PIJ as the former has not merely employed hackers, encryption, and measures of countersurveillance but also used reconnaissance drones in battle, and media bureaus for the dissemination of information and propaganda. Furthermore, the Zapatista National Liberation Army (EZLN) in Mexico, when penned into inaccessible jungle and mountain regions under constant pressure from the Mexican army, exploited the possibilities provided by the cyber-infrastructure to disseminate information, which proved crucial for the movement's survival (Jordan and Taylor 2004, 92–93). In addition, the Chinese government has in the past employed both civilian and semicivilian hacker groups as proxies when engaging in espionage (Elegant 2009). Last, the Kremlin-affiliated hacker group Fancy Bear has engaged in cyber espionage against agencies with strategic importance to the Russian government (Stone 2016).

That does not mean that the conceptualization of the "proto-state hacker" is without limitations, and as with any ideal type its difficulties lie in the inclusion of a vast number of diverging beliefs, ideologies, inspirations, past grievances, future hopes, practices, and strategies. For example, will the "proto-state hacker" of PIJ necessarily share the features of a "proto-state hacker" in Mexico? Conversely, will the proto-state hacker subordinated in a *military* hierarchical movement necessarily share the same features as the "proto-state hacker" in a *nonviolent* hierarchical movement? Indeed, if the "proto-state hacker" of PIJ becomes "proto-state" in terms of emulating the features of a modern state army, can one imagine a qualitatively different actor becoming "proto-state" by emulating a different set of state features (economic, information-based, or service-based)?

The questions derived from the limitations inherent in the proposed category outline some of the issues for future research to focus on. First and most important, comparative research must be initiated to link the "proto-state hacker" of PIJ with other appropriate cases, also those outside the confines of the Middle East. Only by sampling a greater number of similar cases can we nuance the variations, tendencies, and inclinations that the category embodies. Second, future research should delve into the causes for the emergence of the "proto-state hacker." The Israeli matrix of control is an exemplary case to study the dialectic between surveillance and resistance, but it is also an extreme. In a different context and struggle, is there a different dialectic at play than surveillance/resistance that produces the "proto-state hacker"? In addition, does it produce a different type of "proto-state hacker"?

Last, I have compared the capabilities of the electronic unit with advanced nation state hackers, but it is important to note that we still know significantly little about the resources of PIJ's electronic unit and its exact capabilities. For example, does PIJ employ commonly available tools such as the TOR browser or PGP, or does it receive

advanced devices and training from its patrons, such as Iran? If it is the former, I argue that my hypothesis is correct. However, if PIJ in fact employs advanced technology provided by foreign states, it would imply that the electronic unit is far more advanced than a number of economically small states. There is then a need for future research to focus on what tools and devices the proto-state hacker employs.

No matter how we choose to categorize these cyber actors, or what terms we choose to employ to capture the nature of their being and practice, there is little doubt that the current hacker taxonomies must take into account the emergence of electronic units in political hierarchical organizations striving for and consequently emulating statehood. What categories we apply and what meaning these categories signify are subject to continuous development and modification. Indeed, the need for understanding the actors engaging in this development underscores the need for a precise categorization, and the introduction of the "proto-state hacker" is a first attempt at doing so.

Declaration of Conflicting Interests

The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author received no financial support for the research, authorship, and/or publication of this article.

Notes

1. The fieldwork was carried out as a part of an earlier project on the digitization of the Palestinian resistance. The fieldwork carried out in the West Bank also included interviews with other armed movements such as Hamas, the Popular Front for the Liberation of Palestine (PFLP) and the al-Aqsa Martyrs' Brigades, the armed wing of Fatah (For an elaboration, see Skare 2016). In my analysis of the magazine *Muqatil al-Saraya*, I have assessed how Palestinian Islamic Jihad (PIJ) sees technology and its use, whether it reports operations carried out by its electronic unit, and how it perceives its Israeli counterpart in the digital realm. Insofar as Arabic sources are employed, all translations are mine.
2. As there are a number of taxonomies, I limit myself to the taxonomies of Rogers (2006), Hald and Pedersen (2012), and Seebruck (2015) as Rogers (2006) is referenced extensively and is further developed by other scholars in the field. I refer to Hald and Pedersen (2012) as they update the taxonomy of Rogers (2006) by introducing terms and categories more widely employed by both hackers and security researchers. Last, I refer to Seebruck (2015) as he takes the introduction of socially and politically motivated hackers into account in his taxonomy.

References

Abu Amer, Adnan. 2015. "Hamas' Cyber Battalions Take on Israel." *Al-Monitor*, July 29.

Ackerman, Gwen, and Ilya Khrennikov. 2017. "Honey Trap Exposes Israeli Army's Vulnerability to Social Media." *Bloomberg Technology*, April 3. https://www.bloomberg.com/news/articles/2017-04-03/honey-trap-exposes-army-s-vulnerability-to-social-media-risks.

Ahronheim, Anna. 2017. "IDF Official: Cyber Attack Would Be More Harmful than a Missile." *The Jerusalem Post*, May 14. http://www.jpost.com/Israel-News/IDF-cyber-network-not-affected-by-global-hacking-attack-490701.

Andrejevic, Mark. 2016. "The Pacification of Interactivity." In *The Participatory Condition in the Digital Age*, edited by Darin Barney, Gabriella Coleman, Christine Ross, Jonathan Sterne, and Tamar Tembeck, 187–206. Minneapolis: University of Minnesota Press.

Bauman, Zygmunt, Bigo Didier, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, and Rob B. J. Walker. 2014. "After Snowden: Rethinking the Impact of Surveillance." *International Political Sociology* 8 (2): 121–44.

Bob, Yonah Jeremy. 2017. "Islamic Jihad Master Drone Hacker Convicted in Plea Bargain." *The Jerusalem Post*, January 30. http://www.jpost.com/Israel-News/Islamic-Jihad-master-drone-hacker-convicted-in-plea-bargain-480006.

Coleman, Gabriella E. 2017. "From Internet Farming to Weapons of the Geek." *Current Anthropology* 58:91–101.

Coleman, Gabriella E., and Alex Golub. 2008. "Hacker Practice: Moral Genres and the Cultural Articulation of Liberalism." *Anthropological Theory* 8 (3): 255–77.

Dafoe, Allan. 2015. "On Technological Determinism: A Typology, Scope Conditions, and a Mechanism." *Science, Technology, & Human Values* 40 (6): 1047–76.

David, Steven R. 2002. "Fatal Choices: Israel's Policy of Targeted Killings." *Ethics & International Affairs* 17 (1): 111–26.

Deleuze, Gilles. 1992. "Postscript on the Societies of Control." *October* 59:3–7.

Dencik, Lisa, and Jonathan Cable. 2017. "The Advent of Surveillance Realism: Public Opinion and Activist Responses to the Snowden Leaks." *International Journal of Communication* 11:763–81.

Dencik, Lisa, Arne Hintz, and Jonathan Cable. 2016. "Towards Data Justice? The Ambiguity of anti-surveillance Resistance in Political Activism." *Big Data & Society* 1:1–12.

Elegant, Simon. 2009. "Cyberwarfare: The Issue China Won't Touch." *Time*, November 18. https://content.time.com/time/world/article/0,8599,1940009,00.html.

Foucault, Michel. 1990. *The History of Sexuality: An Introduction*. London: Penguin Books.

Foucault, Michel. 1994. "The Punitive Society." In *Ethics: Subjectivity and Truth*, edited by Paul Rabinow, 23–38. New York: The New Press.

Fuchs, Christian. 2011. "WikiLeaks: Power 2.0? Surveillance 2.0? Criticism 2.0? Alternative media 2.0? A Political-economic Analysis." *Global Media Journal: Australian Edition* 5 (1): 1–17.

Hald, Sara L. N., and Jens M. Pedersen. 2012. "An Updated Taxonomy for Characterizing Hackers According to Their Threat Properties." Presentation at 14th International Conference on Advanced Communication Technology, PyeongChang, South Korea, February 19–22.

Halper, Jeff. 2015. *The War against the People: Israel, the Palestinians and Global Pacification*. London: Pluto Press.

Harcourt, Bernard.2015. *Exposed. Desire and Disobedience in the Digital Age*. Cambridge: Harvard University Press.

Harris, Emily. 2015. "In the West Bank, Facebook Posts Can Get You Arrested, or Worse." National Public Radio, June 18. https://www.npr.org/sections/parallels/2015/06/18/415189087/in-the-west-bank-facebook-posts-can-get-you-arrested-or-worse.

Hintz, Arne. 2012. "Challenges to Freedom of Expression in the Digital World: Lessons from WikiLeaks and the Arab Spring." *Journal of Communication Studies* 5 (1): 83–105.

Hintz, Arne, and Lisa Dencik. 2016. "The Politics of Surveillance Policy: UK Regulatory Dynamics after Snowden." *Internet Policy Review* 5 (3): 2–16.

Hintz, Arne, Lisa Dencik, and Karin Wahl-Jorgensen. 2017. "Digital Citizenship and Surveillance Society: Introduction." *International Journal of Communication* 11:731–39.

Hroub, Khaled. 2004. "Hamas after Shaykh Yasin and Rantisi." *Journal of Palestine Studies* 33 (4): 21–38.

Jordan, Tim, and Paul Taylor. 2004. *Hacktivism and Cyberwars: Rebels with a Cause?* London: Routledge.

Kane, Alex. 2016. "Post, Share, Arrest: Israel Targeting Palestinian Protestors on Facebook." *The Intercept*, July 7. https://theintercept.com/2016/07/07/israel-targeting-palestinian-protesters-on-facebook/.

Karatzogianni, Athina. 2017. "Leaktivism and Its Discontents." *Bepress*, September 11. https://works.bepress.com/athina_karatzogianni/30/download/.

Karatzogianni, Athina, and Martin Gak. 2015. "Hack or Be Hacked: The Quasi-totalitarianism of Global Trusted Networks." *New Formations* 84 (84–85): 130–47.

Karatzogianni, Athina, and Andrew Robinson. 2014. "Digital Prometheus: WikiLeaks, the State–Network Dichotomy, and the Antimonies of Academic Reason." *International Journal of Communication* 8:2704–17.

Kuntsman, Adi, and Rebecca L. Stein. 2015. *Digital Militarism: Israel's Occupation in the Social Media Age*. Stanford: Stanford University Press.

Lay, Maxwell G. 1992. *Ways of the World: A History of the World's Roads and of the Vehicles That Used Them*. New York: Rutgers University Press.

Lyon, David. 2014. "Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique." *Big Data & Society* 1 (2): 1–13.

McChesney, Robert. 2013. *Digital Disconnect: How Capitalism Is Turning the Internet against Democracy*. New York: The New Press.

Muqatil al-Saraya. 2013. "Information Security." July, 11–12. https://files.saraya.ps/2013/mokatel_alsaraya11.pdf.

Pötzsch, Holger. 2015. "The Emergence of iBorder: Bordering Bodies, Networks, and Machines." *Environment and Planning D: Societies and Spaces* 33 (1): 101–18.

Rogaway, Phillip. 2015. "The moral character of cryptographic work." Presentation at Asiacrypt 2015, Auckland, New Zealand, December 2.

Rogers, Marcus K. 2006. "A Two-dimensional Circumplex Approach to the Development of a Hacker Taxonomy." *Digital Investigation* 3 (2): 97–102.

Samuel, Alexandra W. 2004. "Hacktivism and the Future of Political Participation." PhD diss., Harvard University, Cambridge.

Seebruck, Ryan. 2015. "A Typology of Hackers: Classifying Cyber Malfeasance Using a Weighted Arc Circumplex Model." *Digital Investigation* 14:36–45.

Skare, Erik. 2016. *Digital Jihad: Palestinian Resistance in the Digital Era*. London: Zed Books.

Smith, Lydia. 2017. "Israel Police Mistakenly Arrest Palestinian Man for Writing 'Good Morning' on Facebook." *Independent*, October 23. http://www.independent.co.uk/news/uk/home-news/israel-police-palestinian-man-arrest-good-morning-facebook-page-translation-mistake-a8015626.html.

Stone, Jeff. 2016. "Meet Fancy Bear and Cozy Bear, Russian Groups Blamed for DNC Hack." *The Christian Science Monitor*, June 15. https://www.csmonitor.com/World/Passcode/2016/0615/Meet-Fancy-Bear-and-Cozy-Bear-Russian-groups-blamed-for-DNC-hack.

The RSA. 2011. "The Internet in Society: Empowering or Censoring Citizens?" YouTube, March 14. https://www.youtube.com/watch?v=Uk8x3V-sUgU.
Tufekci, Zeynep. 2014. "Social Movements and Governments in the Digital Age: Evaluating a Complex Landscape." *Journal of International Affairs* 68 (1): 1–18.
Tufekci, Zeynep. 2017. *Twitter and Tear Gas: The Power and Fragility of Networked Protest*. New Haven: Yale University Press.
van der Velden, Lonneke. 2015. "Leaky Apps and Data Shots: Technologies of Leakage and Insertion in NSA-surveillance." *Surveillance & Society* 13 (2): 182–96.
Weizman, Eyal. 2007. *Hollow Land: Israel's Architecture of Occupation*. New York: Verso Books.
Zajácz, Rita. 2013. "Wikileaks and the Problem of Anonymity: A Network Control Perspective." *Media, Culture & Society* 35 (4): 489–505.

Author Biography

Erik Skare is a doctoral research fellow at Department of Culture Studies and Oriental Languages, University of Oslo, where he is preparing his doctoral dissertation on the history of Palestinian Islamic Jihad. He has previously published the book *Digital Jihad: Palestinian Resistance in the Digital Era* (Zed Books 2016) on Palestinian hackers and the digitization of the Palestinian resistance.