Manipulating uncertainty: cybersecurity politics in Egypt

Hassib, B.; Shires, J.

JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2021, 1–16
doi: 10.1093/cybsec/tyaa026
Research Paper

Research Paper

Manipulating uncertainty: cybersecurity politics in Egypt

Bassant Hassib[1] and James Shires [2]

[1]Department of Political Science, British University in Egypt, Suez Desert Road, El Sherouk City, Cairo, 11837, Egypt and [2]Institute of Security and Global Affairs, University of Leiden, Turfmarkt 99, Den Haag, 2511DP, The Netherlands

Correspondence address. Institute of Security and Global Affairs, University of Leiden, Turfmarkt 99, 2511DP Den Haag, The Netherlands; Tel: +31 70 800 9090, E-mail: j.shires@fgga.leidenuniv.nl

Received 1 July 2020; revised 2 November 2020;

Abstract

Cybersecurity, defined as the prevention and mitigation of malicious interference with digital devices and networks, is a key area of contest for digitalized politics, especially in uncertain and turbulent situations. Nowhere is this more starkly illustrated than in states such as Egypt, where the period since the January 2011 revolution has seen several changes of government and the subsequent consolidation of executive power, increasingly strict limits on free speech, and extensive violence by Islamist groups against the state and civilian targets and by the state against protesters and dissidents. How, then, are cybersecurity policies, practices, and technologies deployed and contested in uncertain political environments? The article argues that cybersecurity provides a way for the Egyptian government and opposition activists to "manipulate uncertainty" to their advantage. Each side uses cybersecurity policies, practices, and technologies to restrict their adversary's scope for action, seeking to make the other more predictable while retaining or increasing their own freedom of action. In addition to providing extensive empirical data on cybersecurity developments in Egypt, the article makes two theoretical contributions. First, it shows how political struggles between state and opposition movements assimilate the influential language and content of cybersecurity, generating distinct cybersecurity politics. Second, it highlights the role of uncertainty as a driver—among others—of cycles of innovation and response in contentious politics, including those that center on cybersecurity.

Key words: cybersecurity; Egypt; uncertainty; contentious politics; surveillance; censorship

Introduction

Individuals, organizations, and states all seek to protect themselves, their communications, and their data from a variety of threats online, including fraud, data leaks, disruptions to online services, and corporate and national surveillance. Cybersecurity, defined as the prevention and mitigation of malicious interference with digital devices and networks, is highly politicized and a key area of contest for digitalized politics, especially in uncertain and turbulent situations [1].

Nowhere is this more starkly illustrated than in states such as Egypt, where the period since the January 2011 revolution has seen several changes of government and the subsequent consolidation of executive power, increasingly strict limits on free speech, and extensive violence by Islamist groups against the state and civilian targets and by the state against protesters and dissidents. The current Egyptian government, under President Abdel Fattah Al-Sisi, has introduced and extended laws on terrorism, media, and cybercrime, created specialist national and regional bodies for cybersecurity, and invested in and experimented with new techniques and technologies of digital surveillance [2, 3]. Political activists and protesters have changed tactics in response, countering government pressure by moving between various platforms and experimenting with different means of organization, mobilization, and communication [4, 5]. This article thus draws on events in Egypt to ask: how are cybersecurity policies, practices, and technologies deployed and contested in uncertain political environments?

The article argues that cybersecurity is a way for the Egyptian government and opposition activists to "manipulate uncertainty" to their advantage. Each side uses cybersecurity policies, practices, and technologies to restrict their adversary's scope for action, seeking to make the other more predictable while retaining or increasing their own freedom of action. In other words, each side uses cybersecurity to make the other uncertain about their actions while increasing their certainty about the other's actions. This manipulation of uncertainty revolves around access to and secrecy of information, techniques, and technologies of (counter)surveillance and censorship, as well as broader communications law and policy. In these processes of manipulation, "cybersecurity" is a highly malleable term; not necessarily referring to any specific infrastructures or practices but deployed strategically throughout the wider field of digital politics.

This argument builds on extensive scholarship on the role of digital media in contentious politics and social movements, as well as recent works in cybersecurity and political science that understand states and societies as information systems, detailed in the following sections. In addition to providing extensive empirical data on cybersecurity developments in Egypt, it makes two theoretical contributions. First, it shows how political struggles between state and opposition movements assimilate the influential language and content of cybersecurity, generating distinct cybersecurity politics. Second, it highlights the role of uncertainty as a driver—among others—of cycles of innovation and response in contentious political practices, including those that center on cybersecurity. By doing so, this article identifies and fills a gap between these literatures: from the contentious politics side, a relative lack of attention on the distinct role of cybersecurity and its relationship with political uncertainty; and from the cybersecurity side, on the imbrication of cybersecurity policies and practices in particular institutional and political contexts and struggles.

The article is structured in five sections, as follows. The first two sections provide the theoretical framework. The first section locates this article in wider scholarship on democratic and authoritarian politics, identifying a range of strategies for manipulating uncertainty available to political actors. The second section moves from a static exploration of different strategies to an examination of their dynamics, drawing on literature in contentious politics to detail how these strategies interact. The third section details the methodology for the empirical data collection, and the fourth section explores the emergence of cybersecurity in Egyptian politics, drawing on laws, policy, and media reports in English and Arabic, as well as interviews with local cybersecurity activists and experts and first-hand experience of events by the authors. The fifth section draws theoretical lessons from this overview, highlighting how repertoires of contention, in Tilly's phrase, have, in the digital age, come to include repertoires of manipulating uncertainty through cybersecurity [6].

Authoritarianism, uncertainty, and cybersecurity

The varied "Arab Spring" protests and revolutions in 2011 are often cited as paradigm examples of the transformational power of Internet politics, although scholars have reached differing conclusions on the extent to which new communications technologies enabled and shaped these events [7–10]. After the wake of the Arab Spring failed to meet expectations of democratization, analyses have shifted from highlighting the organizational and mobilization potential of social media "liberation technologies" [11], to exploring their co-option and exploitation for repression; in Gunitsky's memorable phrase, "corrupting the cyber commons" [12]. Recent mass mobilizations in Sudan, Algeria, Iraq and Lebanon have again raised the salience of the "Arab Spring" frame and resurrected positive representations of social media and political action [13, 14]. In this changing context, we seek to navigate between naivete and dystopia to focus carefully on the way political dynamics shape and are shaped in complex ways by digital media.

The ubiquity of communications across digital devices means that the control of Internet networks is an increasingly crucial aspect of state power and international politics [15–17]. Farrell and Schneier have taken the centrality of information politics in the Internet age further, reading states as fundamentally information systems [18, 19]. They suggest that the classic democratic/authoritarian distinction can be understood as a difference in the distribution of information: in a democracy, information is more widely spread and of a higher quality (trustworthy, reliable), while in authoritarian states, reliable information is rare, and its dissemination closely controlled.

This conceptualization places information circulation—and therefore uncertainty—at the heart of politics, echoing earlier works focusing on uncertainty in democratic transitions [20]. In Bunce's summary, in democracies the political process is certain and the outcome is uncertain, while in authoritarian states the political process may be uncertain but the outcome certain [18, 21]. Of course, this is a simplification, because political processes are as much a part of the contest as outcomes; as Schedler explains, political actors are simultaneously uncertain about the location of the game, the rules—and metarules—of the game, and the score [22]. But the general point holds, even as a matter of degree: certainty about process is higher in more democratic states, and certainty about outcome in more authoritarian states.

However, political actors do not merely orient their action around uncertainty but manipulate uncertainty to achieve strategic goals. As Lynch *et al.* argue in their study of post-2011 Egyptian online political clusters, elites can strategically promote or diminish uncertainty, as can organize opposition groups [23]. The manipulation of uncertainty appears clearly in accounts of securitization: while a threat can be magnified by exaggerating its potential damage, it can also be magnified by making it uncertain, appearing liable to happen at any time through discourses of imminence and "unknown unknowns" [24–26]. Uncertainty is therefore not just a feature of the world or a specific political system (how likely is information to be true, how likely is a certain action to lead to specific consequences), but is also something over which one can exert control for political gain.

More specifically, we can distinguish between the subjective uncertainties of those in power and those seeking change. Although in hybrid or authoritarian systems the incumbent is highly likely to remain in office throughout a critical political juncture (a referendum, protests, constitutional change, parliamentary elections, and so on), there always remains some uncertainty for those in power—subjectively much more so than may appear from the outside—and so they usually seek to overdetermine their continued grasp on power [27–29]. In contrast, opposition activists continue to seek change even when it seems clearly unfathomable; indeed, the story of many social movements, including Egypt's 2011 January revolution, is of no-one quite believing it would happen until it did, and yet continuing nonetheless [30]. In short, activists often possess hope and faith despite their fear, and against the balance of

Table 1: Strategies for manipulating uncertainty

Actor strategies	
Minimize or manage own uncertainty	*Maximize or exploit adversaries' uncertainty*
Gather data and build predictive capability	Control and keep information secret
Limit action space	Act erratically or unpredictably
Implement multiple overlapping systems	Communicate vaguely or ambiguously

probabilities [31]. We can summarize these subjective uncertainties as paranoid and optimistic, respectively, each deviating in opposite directions from an "objective" view of uncertainty in the state qua information system [32, 33]. Complicating the matter is the issue of second-order beliefs: the activist believes the dictator to be paranoid while the dictator believes the activist to be unduly optimistic, and these beliefs about the other feed back into their subjective judgment of uncertainty [32, 33].

The manipulation of uncertainty can thus be targeted at specific actors or groups, rather than the population in general. Combining the two insights on manipulation and subjective uncertainty above suggests that both incumbent elites and opposition seek to diminish their own subjective uncertainty rather than the uncertainty *per se* around political events, while increasing uncertainty for their opponents. Furthermore, subjective uncertainty can not only be increased or decreased, but can also be managed or exploited. Scholarship on risk as a social organizing principle holds that actors, in politics and elsewhere, are fundamentally concerned not just with calculating risk, but also with risk management strategies that accept high levels of uncertainty and seek to achieve strategic goals in a highly uncertain environment [34, 35]. Together, these insights enable us to identify six actor strategies for manipulating uncertainty, as summarized in Table 1, and elucidated in the following paragraphs.

The first three strategies, in the left-hand column, seek to minimize or manage the subjective uncertainty of the actor themselves (whether incumbent elite or political opposition), as follows. First, gathering data to better predict events is the most intuitive way of minimizing uncertainty. As risk scholars show, however, there is an important distinction between the act of prediction and the ability to make accurate predictions; a supposedly predictive apparatus does not necessarily need to be proven accurate in order to minimize subjective, rather than objective, uncertainty [36]. A second way of minimizing uncertainty is to limit the space for action overall. If fewer possibilities for action are perceived to be available, then subjective uncertainty decreases even without greater predictive power. As the literature on deterrence and coercion in international relations demonstrates, governments regularly deploy a wide range of strategies that seek to narrow the decision space of adversarial interaction, for themselves and others [37, 38]. The third strategy in this column manages, rather than minimizes, an actor's subjective uncertainty by creating multiple overlapping systems. Scholarship on risk and resilience identifies redundancy as a core risk management practice, although here again it is the perception of redundancy, rather than a genuine ability to function whatever the situation, that manages an actor's subjective uncertainty [39–41].

The second three strategies, in the right-hand column, seek to maximize or exploit the subjective uncertainty of an adversary. First, in the inverse of gathering data to minimize uncertainty, an actor can maximize an opponent's uncertainty through secrecy, restricting their access to relevant information. The importance of secrecy to political action is recognized in a range of disciplines [42, 43], and its effect of increasing uncertainty for opponents has been highlighted in instances of decisive deception in international politics [44]. A second strategy of maximizing an adversary's uncertainty is to act erratically or unpredictably, widening the action space rather than restricting it. Again, surprise and unpredictability is a tactic long regarded as crucial in both conventional and asymmetric conflicts, also usefully deployed in domestic political struggles [45]. Some commentators even suggest that adopting a metastrategy of general unpredictability—in other words, lacking a strategy—can be as effective as seeking to be unpredictable in specific instances [46]. The third and final strategy seeks to exploit rather than maximize uncertainty by communicating in a vague or ambiguous manner, following international relations literature on "strategic ambiguity" [3, 47, 48].

These six strategies are ways in which political actors can manipulate uncertainty to their advantage. In outlining these six strategies, we do not mean to suggest that they are an exhaustive list, but merely the most likely ways of manipulating uncertainty appearing across several theoretical literatures. It should be stressed also that there are many causes, strategies, and repertoires of political action that do not have the sole or part aim of manipulating uncertainty, and it is beyond the scope of this article to review all of them [6, 49].

Where does cybersecurity fit into this account of political actors manipulating uncertainty for their own ends? Cybersecurity, as a security issue, is fundamentally concerned with uncertainty [50]. Many approaches to cybersecurity are based on risk reduction, as various risks to digital networks are identified and managed through technosocial mechanisms of prevention, regulation, insurance, and compensation [51]. However, there is also substantial uncertainty about the appropriate content and scope of cybersecurity. The field of cybersecurity has evolved from narrow and largely technical notions of information security to become a highly politicized and sprawling term [52, 53]. It includes state and commercial espionage, cyberattacks that cross the threshold for "acts of war," privacy and data collection, disinformation and foreign interference in domestic politics, and cybercrime as both technologically-enabled fraud or "computer misuse" and as content-based transgressions of political or social boundaries.

Consequently, cybersecurity is a highly malleable term, as we have argued in previous settings, with multiple interpretations and a sprawling set of meanings [1, 3, 54, 55]. One of the key tensions in defining cybersecurity is in whether it concerns only technological intrusions into networks, preserving technical properties of confidentiality, integrity, and availability of data, or whether it also involves the management and control of content moving through those networks: in short, whether it protects the medium or the message [56]. More broadly, cybersecurity concerns simultaneously unarguable yet difficult to define risks, changing rapidly with technological developments [57–59]. This flexibility means that policies and technologies bearing the label of "cybersecurity" are ideal candidates for political strategies aimed at manipulating uncertainty.

Studies of cybersecurity in the Gulf states [60, 61] and in Turkey [62] suggest that cybersecurity is redefined and exploited by a range of domestic political actors to gain or retain power. These studies prise apart conventional understandings of a bipolar split internationally between states supporting "cybersecurity" and "information security," showing that both can exist simultaneously in a single state [3]. We expand the conclusions of these related regional studies to show how various political actors in Egypt draw on cybersecurity to manipulate uncertainty in the fourth section of this article; in the next section, we move our theoretical discussion from a static examination of strategies to explore the dynamics of uncertainty.

The dynamics of uncertainty in digital politics

Contentious politics deals with repertoires and dynamics, not static strategies. Political action takes place in specific contexts, in response to and seeking to succeed against specific opponents [6]. A dynamic or relational approach to contentious politics often revolves around a "nexus" between repression and—depending on the scholar—dissent, protest, mobilization, and/or conflict [63, 64]. The identification of a nexus highlights how actions on both sides impact the other, thereby shaping the overall trajectory of political contest—and, at times, requiring spontaneous action to redirect such interactions toward or away from violence [65]. Such actions include both direct contest and alternatives: e.g., choosing not to protest, or, for states, "accommodating" opposition factions. This dynamic approach has been formulated systematically as "strategic interactionism," explored by Jasper and Duyvendak among others [66, 67]. Scholars have applied these conceptual frameworks to various aspects of contentious politics in Egypt, including the mobilization and repression of Islamist movements [68]. This field of study also emphasizes the disaggregation of the state, aligning with longer views of the tension between military, intelligence, and presidential powers in Egypt [29, 67].

However, scholars of strategic interactionism and contentious politics have largely omitted cybersecurity as a site of contestation; e.g., the otherwise excellent volume on protest dynamics across the "Arab Spring" countries by Volpi and Jasper does not address cybersecurity at all, with social media as a background technological transformation, rather than a site of contestation [69]. This article seeks to rectify this omission. In doing so, it draws on research connecting contentious politics, authoritarian practices, and "data activism," both in the Middle East (e.g., Iran [70]) and more widely [71]. Although this body of work also avoids direct engagement with the concept of cybersecurity, it provides a more sophisticated theoretical underpinning for the examination of digital politics—including, as detailed below, questions of surveillance and creative resistance.

As with contentious politics, offensive and defensive developments in cybersecurity are dynamic, context-dependent, and adversarial. Offensive and defensive actions only succeed or fail in specific contexts, exemplified by repeated exhortations to cybersecurity defenders to "understand the threat actor," on the one hand [72], and, conversely, findings that one of the characteristics of advanced threats—and the mark of a successful penetration tester—is time spent on target-specific reconnaissance [73]. Overall, this phenomenon creates a "cat-and-mouse" characteristic in cybersecurity, where improvements in defense motivate offensive adaptations to overcome those improvements, and vice versa [74].

Moving to repertoires and dynamics, rather than static strategies, means that the overview of strategies for manipulating uncertainty laid out in the first section of the article is not sufficient, and we also need to ask: how do these strategies interact? We can theorize this interaction using the division between two sets of strategies above: the first managing or minimizing subjective uncertainty of the actor, and the second maximizing or exploiting that of the opponent. Rather than conceptualizing these two sets of strategies all as options available to a single actor, we can also view them as responsive moves by adversarial actors. More fully, actors minimize and manage uncertainty in response to and in the context of adversaries seeking to maximize and exploit that actor's uncertainty, and conversely aim to maximize and exploit uncertainty for specific adversaries while aware that these adversaries are seeking to manage and minimize their own uncertainty.

We can therefore see the three rows of Table 1 as three separate dynamics of uncertainty in digital politics, which we refer to as surveillance/countersurveillance, censorship/creativity, and redundancy/ambiguity. These dynamics are represented in Table 2 below, which repeats Table 1 but adds a third column (the left-hand column) for the three dynamics above. The rest of this section explains these dynamics and places them in their theoretical context, justifying our description of each and the distinction between them.

Before exploring each dynamic in turn, we first stress that—like Table 1—this is not an exhaustive list, not least because it only concerns digital informational politics. There are of course other dynamics of uncertainty outside digital politics: e.g., many ways to limit physical spaces of action are not treated here [10], as we are concerned mainly with those dynamics that take place within or involve online networks. We do consider overlaps, e.g., where physical restrictions such as stop and search of devices by security agencies lead to different practices for activists going to join protests. Dynamics of uncertainty can also take place in "offline" information politics, through forms of communication that do not use digital networks or the Internet. Again, we do not consider these here unless they overlap with digital politics. Furthermore, the three dynamics considered here do intersect, often at a technological level: e.g., deep packet inspection technologies can enable both online censorship and surveillance, depending on their configuration.

Regarding the first dynamic, both governments and opposition activists gather data about the other and seek to keep their own information secret, but the surveillance/countersurveillance dynamic that this creates is far from equal. State surveillance is prevalent worldwide and is enabled by a massive societal surge in the generation, collection, and analysis of data in the last two decades,

Table 2: Dynamics of manipulating uncertainty

Dynamic	*Actor strategies*	
	Minimize or manage own uncertainty	*Maximize or exploit adversaries' uncertainty*
Surveillance/countersurveillance	Gather data and build predictive capability	Control and keep information secret
Censorship/creativity	Limit action space	Act erratically or unpredictably
Redundancy/ambiguity (?)	Implement multiple overlapping systems	Communicate vaguely or ambiguously

fundamentally connected to the development of the Internet [75–77]. Some scholars have suggested that the Internet architecture itself enables state surveillance, and could be reconfigured to make it more difficult for states to access information on citizens that contravenes human rights standards [78, 79]. All political actors operate within this wider circulation of data and data products, and so both states and citizens are imbued with a “global culture” of surveillance—the set of assumptions, references, and expectations that accompany a constantly-monitored life—as well as specific surveillance cultures that differ according to sector and geographic location [80]. States generally attempt to keep surveillance architectures secret to prevent their targets evading them, but this is increasingly difficult in an age of megaleaks and the decreasing “half-life” of secrets [43]. Most notably, the Snowden disclosures accelerated a transfer of surveillance from liberal democratic states, where they existed within (however much they subverted) substantial checks and balances, to authoritarian states without any such restrictions against their use in facilitating repression [81–83].

On the other side of the coin, the act of watching and recording is integral to standard accounts of the role of nongovernmental organizations (NGOs) and human rights activists in international politics, and more generally opposition movements that have limited access to or deliberately forgo other methods of contest. Finnemore and Sikkink’s classic account of “naming and shaming” in human rights advocacy requires first the ability to observe and record the actions of governments [84], obscuring its reliance on a wider culture of surveillance in which transparency and the collection of minute-level data are common practices. This (digital) watching and recording are not usually considered as sur-veillance (watching from above), due to power asymmetries in favor of the state against such groups. Consequently, the term sous-veillence (watching from below) has been coined to denote distributed data collection and storage in cases where the individual is acting against the state, like recording devices and wearable cameras [85–87].

In terms of secrecy, resistance to state digital surveillance can be cultivated through personal practices, and many activists rely on a range of technologies to sabotage/block surveillance [88–90]. They have assistance in this from large technology multinationals, whose professed corporate ethos on privacy and diplomatic relationships with liberal states (which diverged significantly in the wake of the Snowden disclosures) have led them to implement extensive antisurveillance measures, such as end-to-end encryption [91]. This is not always the case: the same companies remain cooperative with government surveillance practices in more important commercial markets, and privatized digital surveillance industries create what some have called a “cyber-military-industrial complex” [92].

Regarding the second dynamic, the main way states limit the action space online is through censorship and information controls. Scholars have noted how authoritarian states such as China have progressed through successive “generations” of online information controls, from firewalls and simple filtering, to institutional measures to funnel online activity into acceptable bounds, and finally sophisticated forms of manipulation of content and population sentiment [12, 93]. These generations are cumulative rather than transitional, meaning—e.g.—that states do not stop national-level blocking when they have access to sophisticated targeted capabilities, but instead choose when to use each in different situations. The adoption of information controls, like surveillance software, often depends on “dual-use” commercial traffic management software, originally developed and marketed to corporate organizations, that can be implemented at a national level to extend censorship online [94].

In response to extensive information controls, creativity and surprise are a key part of online protests and political action. Code words or disguised images and videos are common ways to evade online censorship [95]. Longstanding techniques of offline innovation and creativity, such as flash mobs and distributed, decentralized protest actions, have reemerged online, pioneered by the “hacktivist” group Anonymous [96]. Like surveillance/countersurveillance, the dynamic between information controls and online creativity is marked by a significant power differential: elites and governments deploy information controls, while those with less power rely on erratic and unpredictable countercensorship practices. However, cultivating online unpredictability requires effort, and so is unlikely to be widely adopted in populations of varying digital access and literacy, such as Egypt. For most of the population, information controls and surveillance lead to a “chilling effect,” where citizens practice self-censorship to curtail their expression of any ideas they perceive to be critical to ruling institutions or challenging societal norms [97, 98].

The last two strategies in the typology in Table 2—creating multiple overlapping systems and communicating vaguely or ambiguously—lead less clearly to a response/counterresponse dynamic than the first two sets of strategies. These last strategies seek to manage or exploit subjective uncertainties, rather than minimizing or maximizing them, respectively, and so should be considered alongside rather than in addition to the first two dynamics. For example, purchasing multiple surveillance systems with overlapping functionality from different suppliers (as the Egyptian government and others have done with spyware companies Hacking Team and FinFisher, discussed in the following section), might be considered a form of redundancy. Similarly, the concurrent operation of different generations of information controls manages the risk that any particular one will be ineffective, especially when individuals and other states are constantly seeking to circumvent them. On the contrary, communicating vaguely or ambiguously is a complementary strategy to the first two means of maximizing an adversary’s uncertainty: it does not give away secret information (e.g., in the “neither confirm nor deny” statements of many state security agencies) and facilitates erratic and unpredictable action by remaining consistent with multiple possibilities. The “redundancy/ambiguity” dynamic proposed in Table 2 is therefore tentative and accompanied by a question mark, acknowledging the different nature of these strategies.

Finally, what do these dynamics suggest about the role of cybersecurity policies and technologies in manipulating uncertainty? At an abstract level, it seems clear that cybersecurity could be associated with both sides of these dynamics, involving opposing conceptions of threat and vulnerability. For example, cybersecurity justifications could be invoked for the adoption of surveillance technologies by states and for the adoption of countersurveillance technologies by activists, each requiring a different idea of what the cybersecurity threat is, and what should be protected [1]. This question, however, is better answered empirically, and will be addressed in the remainder of the article. To anticipate the following sections, we argue that cybersecurity policies and technologies appear on both sides of the first dynamic, and predominantly on the government side of the second and third dynamics.

Methodology

Methodologically, the empirics of this research are based on a range of primary and secondary sources: relevant national and regional cybersecurity legislative and cooperative frameworks; reports of national, regional, and international digital rights NGOs; surveillance technology tenders; and news articles in English and Arabic. These sources are supplemented by three interviews conducted with prominent Egyptian cybersecurity experts and activists, in addition to the quasi-ethnographic data gathered through one of the authors' lived experiences as an Egyptian national and Cairo resident.

The three interviews were semistructured and took place between early 2018 and mid-2019. Interviews were conducted in person and via emails and VOIPs (Wire and WhatsApp), transcribed, and analyzed qualitatively. The interview questions gathered data on—but not limited to—the following: Egypt's cybersecurity legislation and actors; Egypt's regional and international cooperative frameworks on cybersecurity; Egypt's technologies and capabilities of digital surveillance and censorship; the societal implications of Egypt's cybersecurity policies, practices and surveillance technologies; targets of state surveillance (activists, journalist, NGOs, etc.); cyber norms of digital activism, countersurveillance, sousveillance, censorship circumvention, and digital rights advocacy in Egypt; and networking between tech activists and rights activists on the national regional and international levels. The data gathered from the interviews inform the argument of the article, but is only one source among many used in the following section, and where possible interview data were triangulated with open source data and other fieldwork outside the scope of this article [54, 60]. Due to the risks to interviewees, we do not provide interviewee details other than a broad description, date, and means of interview.

We note that some of this empirical ground has been covered by others answering related questions, most extensively in Fathy's excellent examination of human rights and freedom of expression online in Egypt [99]. Other related works include Grimm *et al.*'s advice on human and digital security in hostile environments, and Radsch's investigation of cyberactivism and citizen journalism in Egypt [5, 100]. While these important contributions examine the way Egypt restricts digital rights to curb opposition, the challenges facing digital activism, and the ways to adapt to or subvert surveillance in Egypt and/or other states in the region, analysis of strategies of the state and/or activists to manipulate the digital space for their advantage is not sufficient in isolation. We take this work further by focusing on how these strategies interact, and, furthermore, exploring this interaction specifically in the site of cybersecurity. As will be clear in the following section, empirical developments around cybersecurity are strongly skewed towards government actions, although not exclusively so. We consider reasons for this imbalance in the subsequent discussion section.

Cybersecurity politics in Egypt

This section provides an overview of political developments in Egypt over the last decade, focusing on cybersecurity policies, institutions, and technologies in the context of sustained political struggles, often violent, between successive governments and opposition movements. It is organized chronologically, split into three periods: 2011–13, 2014–17, and 2018–20. These periods are marked by key political junctures: the first from the January 25 revolution to the military overthrow of President Mohammed Morsi in June 2013 and subsequent violence, the second with the election of current President Abdel Fattah Al-Sisi in 2014 and his first term, and the third from his re-election in 2018 to the beginning of 2020. This is only an overview of a complex and turbulent decade, and so focuses on crucial moments in Egyptian politics while omitting many important developments for reasons of space.

2011–13

Prior to the January 25 revolution, a major shift in the state's approach to cybersecurity followed textile workers' protests at a historic factory in Mahalla—known as the 6 April Movement—in 2008. Opposition groups, often imitating the April 6 movement or with that movement at their core—used the Internet for blogging, tweeting and to organize on Facebook pages and groups [30]. Such events highlighted the political importance of cyberspace, drawing the attention of the regime of former President Hosni Mubarak. By 2009, Egypt already possessed technology that allowed large scale access to telephone networks, provided by the company Nokia Siemens Networks [101]. In 2011, the Huffington Post reported that the Egyptian government had for several years used deep packet inspection (DPI) monitoring technologies produced by an Israeli-origin subsidiary of Boeing, Narus [102]. As we have reviewed in more detail elsewhere, the main legislation relevant to cybersecurity at this point was the 2003 Telecommunication Law, which permits extensive surveillance: it gives state security institutions the authority to control all telecommunication services, resources and administration in the case of general mobilization [2, 60].

These new forms of activism in cyberspace repeatedly mobilized public opinion, notably after the death of Khaled Saeed in police custody in June 2010, paving the way to the 2011 uprising [103]. Individual activists, in connection with NGOs, trade unions, bloggers and opposition groups, used social media platforms, in particular Facebook groups and pages like "We Are All Khaled Saeed," to plan the 25 January protests [104]. The initial purpose of protesting against police abuse later extended to calling for the resignation of Mubarak [10]. In addition, an online campaign mobilized thousands of Egyptians living aboard to return and support the protests [105, 106]. After 18 days of the uprising, Mubarak stepped down and the Supreme Council of Armed Forces ruled for a transitional period until the election of the Muslim Brotherhood (MB) presidential candidate Mohamed Morsi in 2012.

The mass mobilization in 2011 highlighted the potential of cyberspace as an alternative space for political activism and an instrument of democracy. Wary of this potential, several attempts to circumvent the Internet and counter cyber-activism were undertaken by the Egyptian government, the most infamous of which was the blocking of Facebook and Twitter during the initial protests, followed by a 5-day Internet shutdown [107]. This shutdown was probably achieved through phone calls from a government agency to all major ISPs instructing them to stop services, potentially under the Telecommunications Law (although the ISP hosting the stock exchange remained online), and reportedly cost the Egyptian economy around $110 million [108].[1] To circumvent the Internet blackout, Google and Twitter launched a "voice-to-text" software to allow citizens to communicate without the Internet. The software allows online voicemails to be sent out as texts on Twitter using the hashtag #egypt [109]. Following the protests, security agencies targeted and arrested activists who participated in the protests by tracing their phones. To prevent this, protestors started to remove the batteries of their phones in gatherings, while others learned not to even take their phones with them.[2]

The January 2011 events also revealed further details of existing state surveillance. When protestors broke into the headquarters of

[1] A timeline of the communication shutdown in Egypt is available at https://c2.staticflickr.com/4/3198/5814392791_1a39ac54c0_b.jpg

[2] Anonymous MENA cybersecurity expert, interview, July 13, 2019.

the Egyptian security agency State Security Investigations in March 2011, they retrieved and disclosed tenders for targeted surveillance technologies to compromise Skype and email accounts and control targeted devices, namely the "FinSpy" software imported from then UK-based Gamma International (now Germany-based FinFisher) [110]. Additionally, the cooperation of private telecommunication companies with the government to allow monitoring of calls and text messages, reveal user data, install interception and spyware technologies, and block websites, was disclosed [111]. More general repression of social media increased; e.g., later in 2011, a blogger was sent to prison for a Facebook post critical of the military [112]. In 2012, the Egypt government likely purchased security software and devices from the US-based company Blue Coat to censor and monitor online communications [113].

During this period, the main cybersecurity policy change was the publication of Egypt's National ICT strategy in 2012 [114]. The same strategy was later relaunched under Al-Sisi as a 2014–17 rather than 2012–17 strategy, but no other changes were made [115]. The strategy itself is extremely vague regarding the required changes to surveillance regulation in the Telecommunications Law. On the one hand, it states that the 2003 law "contains certain articles that require amendment in line with Egypt's democratic transition that will promote political openness and protect freedom of expression" (p. 9). On the other hand, it also qualifies this aim, claiming to "bring about the desired balance between the considerations of freedom as a fundamental human right and privacy considerations and national security" (p. 33). Consequently, "the availability of information [that] could harm national security of Egypt or the exposure of relations with other countries at risk under the banner of freedom is not acceptable" (p. 33). As we have argued elsewhere, this strategy thus incorporates ambiguously both an expansive definition of national security "and" an abstract endorsement of human rights [3].

The solidarity and optimistic nationalism of the January 2011 events did not last long. Despite Morsi's rise to power through democratic elections, the MB government was widely seen as betraying liberal civil society organizations and activists who opposed their agenda. In what Schmitter and Karl call the "fallacy of electoralism" [116], a naıve dependence on electoral victory as the source of democratic legitimacy led Morsi's government to turn a blind eye to fulfilling other democratic requirements [9]. Furthermore, Sinai emerged as a hub for militant Islamists due to Morsi's reduction of military operations there. This inefficiency and alienation resulted in a series of protests organized on social media platforms by groups like "Copts for Egypt," "the Black Bloc," and "National Salvation Front." Consequently, in January 2013, Morsi reintroduced the emergency law for 30 days. A second mass revolt took place on June 30, 2013, organized by a youth rebel movement "Tamarrod" (rebellion), largely through social media platforms. This mass protest led to the ousting of Morsi on July 3, 2013 after the intervention of the military and a subsequent government decision to declare the MB a banned terrorist organization [117]. Violence continued throughout 2013, especially after military dispersed MB protesters at Rabaa Square in Cairo in August 2013, reportedly killing at least 700 people [10]. Deep divisions appeared within political groups and even families; e.g., a wife reported her husband to the authorities for sharing Facebook posts on the Rabaa protests.[3]

2014–17

Field Marshall Al-Sisi's initial "caretaker" role was legitimized by national presidential elections in 2014. The deteriorating security situation, including actions by MB offshoots or by ISIS's Sinai-based branch Ansar Beit al-Maqdis, helped the military garner support [118]. The state of emergency was reinforced several times, as authorities cracked down on nonviolent dissent and "public opinion was shaped to perceive civic activism as a non-nationalistic endeavor that hinders the government's counterterrorism efforts" [117]. Al-Sisi won the 2014 election by a landslide, with a reported 96.91% of the votes. In 2014, the government established the Supreme Cybersecurity Council with a committee tasked with monitoring cyberspace for any "deviant" public opinion and "terrorism" content, with no specific definition of these terms [2]. This committee was described as a counterterrorism and counterextremism tool that complemented military operations in Sinai [119, 120]. The online public sphere faced additional suppression, especially of negative portrayals of the new President: e.g., bloggers were arrested and sentenced to prison in 2015 for posting a satirical picture of Al-Sisi with "Mickey Mouse" ears [121].

The new regime received extensive support from the UAE and Saudi Arabia, in contrast to Qatar's support for the MB government, a change reflected in purchases of surveillance technologies. In 2014, France reportedly sold a surveillance system built by Nexa Technologies to the UAE, which was then sent to Egypt as a gift under the codename "Tobleron" [122]. At the same time, a tender for social media surveillance technologies for the Ministry of Interior (MoI) through Systems Engineering Egypt, a local affiliate company of Blue Coat, was leaked [123]. Importantly, these new surveillance technologies were understood as cybersecurity protections, reportedly falling under a broader plan named the "Social Networks Security Hazard Monitoring Operation (public opinion measurement system)" [124]. However, the actual usage of mass surveillance software is still uncertain. According to an Egyptian cybersecurity expert, the security apparatuses do not have the required capacity, in terms of the number of skilled/active personnel and available time, to effectively run such systems.[4]

Government investment in targeted surveillance technologies also increased during this period. In 2015, Privacy International released details of a contract between the Egyptian government and Italian targeted surveillance supplier Hacking Team [101]. According to this report, Hacking Team sent a contract for their software in January 2015 to the Technical Research Department (TRD), a subsection of the Egyptian intelligence agencies who are associated with extensively catalogued human rights violations including torture and mistreatment as well as suppression of political opposition. An interview with an Egyptian cybersecurity expert suggested that Egyptian authorities may have used this software to surveil Italian PhD student Guilio Regini prior to his torture and murder in January 2016.[5]

In this period, the government also introduced broad new laws and policies to limit online dissent. The 2015 Counterterrorism Law authorized state control over digital media, enabling it to shut down websites and monitor online communication [117]. Cyberterrorism is not explicitly defined in the text of the law; however, any online activities related to terrorism are criminalized, including the use of the Internet to learn any techniques that could be used to commit terrorist crimes. The law also prosecutes publishing "fake news" on terrorist attacks or counterterrorism operations if they contradict

[3] Anonymous Egyptian cybersecurity expert, interview, March 26, 2018.

[4] Anonymous MENA cybersecurity expert, interview, July 13, 2019.

[5] Anonymous Egyptian cybersecurity expert, interview, March 26, 2018.

the official statements of the Ministry of Defence. Similarly, the 2016 Law on Regulating the Press and Media, amended in 2018, authorizes the Supreme Council for Media Regulation to monitor the adherence of digital media to public ethics and national security, with the power to block content that may threaten national security [125]. These laws accompanied greater online censorship: by the end of 2016, the Ministry of Interior had closed 163 Facebook pages and arrested 14 Facebook page administrators, while 549 local and foreign news and media websites and platforms critical of the current regime and the status of human rights in Egypt were blocked as of June 2020 [126].

These actions merged counterterrorism and cybersecurity discourses. For example, a progovernment newspaper justified the censorship above using a cybersecurity frame and referring to other governments' efforts in censoring the Internet, including the USA and China, as against "cyber-terrorism" [127]. At a regional level, a Global Centre for Combating Extremist Ideology, named "Etidal" (moderation), was launched in 2017 by the leaders of Saudi Arabia, Egypt, and the USA as a multilateral initiative to combat "cyber-terrorism" and "cyber-extremism" [128]. Similar justifications were also influential in MPs' proposals in 2016 for a national version of Facebook that requires citizen identification for participation [129, 130]. This restriction was justified using the language of cyber threats to national security posed by the right to anonymity and privacy [131]. According to one of the proposals, Egyptian Facebook users would pay a subscription fee to access Facebook, funding a platform and permit-management database run either by Telecom Egypt or the telecoms regulatory agency. Individuals who login to Facebook without subscription would be either fined either 5000 Egyptian pounds, face a 6-month prison sentence, or both [132]. This system, according to the MP, would aid state surveillance in its mission to combat online content that challenges national security [133]. Finally, according to an interview with an Egyptian cybersecurity expert, this period also saw attempts to classify hacktivism as an advanced persistent threat (APT), putting political activism at the top of cybersecurity agendas.[6]

During this period, the Egyptian government also limited access to key Internet censorship circumvention tools such as virtual private networks (VPNs), ostensibly in keeping with wider regional policies [134]. A key example concerns the encrypted messaging application, Signal, which was blocked in December 2016 by the Egyptian and the UAE authorities. In response, and working with Egyptian activists, the creators of Signal updated the application to rely on "domain fronting": using encrypted connections to a popular domain, in this case, owned by Google, to act as a proxy for Signal messages. Further attempts to block Signal in early 2017 inadvertently blocked all Google traffic to Egypt, causing outages and highlighting the technological limitations and experimental character of online censorship in Egypt [135]. More recently, large technology multinationals such as Google and Amazon have decided to prevent domain fronting because it presents a cybersecurity risk, but by doing so making it easier for governments to block Signal and other apps [136]. More broadly, surveillance circumvention tools—with the exception of Wire—remain unpopular in Egypt, despite their availability and easy installation.[7] Some activists have instead turned to alternative platforms, using video games with chat rooms such as League of Legends and World of Warcraft.[8]

Finally, in contrast to cybersecurity acting as a justification for a wide range of online censorship and surveillance, the Egyptian government also became widely seen as a cybersecurity threat to civil society organizations. A Toronto-based interdisciplinary academic institute, The Citizen Lab, has analyzed two phishing attacks against NGOs following accusations of receiving foreign funding without the state's authorization for projects that have "foreign agendas" [137]. These attacks tricked the recipients into providing their personal information and passwords to their work emails and file-sharing accounts. These campaigns were carefully targeted: the first wave impersonated the NGO "Al Nadeem Center for Rehabilitation of Victims of Violence," while the second wave sent a fake link for updates such as detainees' whereabouts or arrest warrants. Another sophisticated tactic observed involves manipulating the two-step verification process on social media and email accounts, and several high-profile activists were targeted by the state in this way [138]. Notably, activist Ola Shohba's personal accounts were compromised in July 2017, and her mobile number for two-factor authentication was deactivated. Shohba argued that the rigid regulations for SIM card registration in Egypt, requiring physical presence with a national ID card, indicate that her mobile phone company cooperated with the Egyptian authorities in enabling this access [139]. Research by Amnesty International in 2020 revealed links between these phishing campaigns and the FinFisher malware noted above; however, it is unclear to what extent these links indicate continued corporate cooperation or, more likely, experimentation with (now publicly available) malware code [140].

2018–20

By the end of Al-Sisi's first presidential term, his former popularity started to fade amid strict economic measures that negatively affected most Egyptians, in addition to intensified crackdown on dissent, freedoms and the civic space. Broad macro-economic trends in Egypt center around a $12 billion loan from the International Monetary Fund (IMF) in November 2016 [141]. One of the key conditions of the IMF loan was floating the Egyptian pound on international currency markets in November 2016, leading to an immediate fall in its value and so increased prices of most commodities: inflation climbed to around 30% in 2017, falling back to 15% in 2018. IMF-imposed measures exacerbated existing structural economic problems, leading the World Bank to describe 60% of Egypt's population as "poor or vulnerable" in July 2019, despite more optimistic government figures released a month later based on an artificially low poverty threshold [142]. New mega-projects, such as the Administrative Capital close to Cairo, still under construction, and the extension of the Suez Canal in 2015, while providing contracts for military agencies [143], added to uncertainty around Egypt's political course [144]. Nevertheless, Al-Sisi was re-elected for a second term in 2018 with a reported 97% of votes, but with a lower turnout. Al-Sisi ran for the election with only one other candidate—who himself is an Al-Sisi supporter—after his main opponent was arrested and all other opposition candidates were prevented from getting on the ballot through intimidation tactics. On the contrary, Al-Sisi's political, economic and security measures were praised by his supporters, citing them as necessary for the preservation of national security [145].

Shortly following Al-Sisi's re-election, a cybercrime law that had been repeatedly re-drafted over the preceding years was approved by the parliament in August 2018. As we have argued elsewhere, the provisions of this law are extremely vague [2, 3]. The Anti-Cyber and Information Technology Crimes Law legalizes surveillance by

[6] Anonymous MENA cybersecurity expert, interview, July 13, 2019.

[7] Anonymous MENA cybersecurity expert, interview, July 13, 2019.

[8] Anonymous MENA cybersecurity expert, interview, July 13, 2019.

requiring Internet service providers to store and provide user's data, the content of the information system, and the equipment used, to the government. It also penalizes websites' administrators if they fail to report to the authorities when they are subject to a cyberattack, and for not taking the precautionary measures to secure their communication, without identifying these measures. The law criminalizes running or using a "website" that incites crime, and broadly defines "website" to include public pages and personal accounts on Facebook, Twitter, and other platforms. It vaguely identifies crimes or the illegal content as activities that might harm the "society's security and cohesion." Egyptian NGOs have argued that the imprecision of terms such as "email" or "website" in the drafting process was an indicator of the legislators' lack of expertise [146]. An interviewee traced this lack of expertise to the deliberate exclusion of relevant legal and technical experts, as well as NGO representatives.[9] Finally, the law stiffens penalties for the same crime if committed using cyberspace, such as calls for protests. This reflects a regional shift under the cooperative framework of the 2010 Arab Convention on Combating Cybercrime, which restricts a wide range of electronic and technical activities [147].

Al-Sisi continued to consolidate power through sweeping constitutional amendments in 2019. The amendments included items on extending presidential term limits until 2024 and allowing him to run for reelection at the end of that term, thereby serving an additional 6-year term until 2030. They also expanded the jurisdiction of military courts over civilians and increased the president's executive powers. Civil society organizations have argued that such amendments narrow the civic space and are a "death knell for democracy" [148]. This period also saw a new National Cybersecurity Strategy, dated 2017–21 and released publicly in December 2018. This new strategy replicated many of the ambiguities of the earlier ICT strategy noted above, highlighting vague threats of cyberterrorism and cyberwarfare, but juxtaposed with proposals for a new national digital identity system like that discussed above [149].

Amid growing dissatisfaction and apathy, in 2019 social media companies revealed and dismantled several progovernment disinformation networks in Egypt. In August 2019, Facebook removed 378 accounts spreading disinformation across the Middle East, tracing the source to media companies "Newave" in UAE and "New Waves" in Egypt [150]. According to the Digital Forensics Research Lab, the manager of New Waves also registered several other organizations in 2017 and 2018, aiming for coordinated amplification of progovernment propaganda across a range of outlets [151]. In September 2019, Twitter removed 271 accounts targeting disinformation against Iran and Qatar, created and managed by a company called "DotDev," again based in UAE and Egypt [152]. A month later, Facebook removed 448 accounts originating in UAE, Egypt and Nigeria, and targeting worldwide, linked to a media company named "Flexell," and 301 accounts promoting the UAE, Saudi Arabia and Egypt and critical of Qatar, Iran, Turkey, originating in Egypt with links to a media outlet named El Fagr [153]. This wave of takedowns followed increased attention on disinformation by Facebook and Twitter due to growing political pressure in the USA, and calls by influential US politicians and academics to treat foreign disinformation as a cybersecurity threat [55].

In September 2019, a former military contractor, Mohamed Ali, went on a social media spree seeking to galvanize people against the military. In a series of videos, filmed in exile, he claimed that Al-Sisi was squandering public funds, directing them toward construction projects led by the military and building grand palaces while the Egyptian public was living in austerity [154]. Subsequent protests were met with "old-fashioned" mass surveillance, as security agencies combined cyberattacks and intensified policing of social media with a random "stop and search" of phones and laptops on the streets [155]. Additionally, NetBlocks technical measurements showed that the government slowed down and temporarily disabled Facebook messenger from allowing people to share locations and pictures during protests. More generally, access to social media became unavailable/intermittent on some ISP networks [156]. To circumvent this, activists and individuals developed new practices before heading to downtown or Tahrir square: deleting political posts and messages that might incriminate them; temporarily deactivating Facebook pages and Messenger; and keeping their phones and laptops signed in with a second "fun" Facebook account free of any political content [155].

More generally, there has been an overall increase in repression due to digital activism in Egypt over the whole decade, reflecting wider trends [157]. A report by the Open Technology Fund cataloguing arrests related to social media and online activism highlights several patterns, including tendencies to repeatedly target well-known activists and focus on sharing specific content (such as the satirical images of Al-Sisi referenced above) [158]. In addition to device seizures, surveillance, and other tactics detailed throughout this section, this report highlights the role of online informants, and an interviewee also noted that journalists have reported each other for their online opinions.[10] Similarly, although progovernment individuals and groups historically countered activists by reporting them to national security organizations, this is no longer necessary. Instead, an individual can join any progovernment group/page on Facebook (such as "*fi hob Al-Sisi*" [Love for Al-Sisi]) and report a specific activist account to the other members of the group, then all the members of the group/page can report this account as abusive or fake to Facebook to be closed.[11] The focus here on the actions of government agencies and a relatively narrow set of opposition activists must therefore be placed in the wider context of polarized political debate and shifting societal expectations about privacy and appropriateness of online debate.

Manipulating uncertainty

The previous section demonstrates that cybersecurity policies, practices, and technologies are a central part of Egyptian politics. There have been protracted political struggles over the introduction of cybersecurity laws and technologies, most clearly evident in leaks around the procurement of surveillance technologies and the 2018 cybercrime law. Multiple interpretations of cybersecurity have emerged in Egyptian politics, from cybersecurity as concerned narrowly with intrusions into networks, to broader associations with individual rights, with privacy as an element and enabler of cybersecurity, as well as cybersecurity as a foundation of national information security. However, this overview also suggests that cybersecurity policies, practices, and technologies are not merely the

[9] Anonymous Egyptian cybersecurity expert, personal communication, January 26, 2018.

[10] Anonymous Egyptian cybersecurity expert, personal communication, March 26, 2018.

[11] Anonymous MENA cybersecurity expert, personal communication, July 13, 2019.

"subject" of political contest but are also political tools, used by those in power and their opposition.

This section analyzes the events detailed above using the theoretical framework of manipulating uncertainty developed in the first two sections. As we argued there, manipulating uncertainty is a well-established goal for both incumbent elites and opposition activists, with some placing the manipulation of uncertainty at the core of political change [22, 23]. We proposed a framework containing two broad ways for an actor to manipulate (subjective) uncertainties: minimizing or managing their own uncertainty and maximizing or exploiting their adversaries' uncertainty. We then expanded this framework to include six paired strategies, creating three overall dynamics for manipulating uncertainty (Table 2, repeated below). The two key questions, therefore, are to what extent Egyptian politics in the last decade involves strategies and dynamics for manipulating uncertainty, and where cybersecurity policies, practices and technologies fit into these strategies and dynamics. In the following paragraphs, we answer these questions for each pair of strategies and their associated dynamic in turn. We do so by combining the theoretical framework of Sections 1 and 2 above with the empirical data in Section 4. This discussion is thus derived from our research, building on the secondary literature on digital politics in Egypt noted in earlier sections.

Before reviewing these strategies, it is important to be clear about the scope of the claims in this section. When we state that an event indicates a strategy of manipulating uncertainty, we do not claim that this is the explicit intent of specific individuals. This would be problematic for several reasons, including the availability of data on the intent of relevant individuals, such as senior government officials, and the reliability of that data—especially as publicly stated intent is rarely an accurate guide to actual decision-making procedures, in Egypt and elsewhere. Most importantly, it would be problematic because most strategic actions achieve multiple goals, especially in complex political arenas.

We, therefore, do not seek to show that manipulating uncertainty is the "only" purpose of cybersecurity policies, practices, and technologies. For example, surveillance technologies (whether targeted or at a national level) do not only minimize uncertainty about opposition activists and their plans, as we argue below; they also help to catch criminals and terrorists according to definitions that would be accepted internationally. On the other side, activists may use new communications technologies with stronger cybersecurity protections not just to keep information secret and maximize government uncertainty about their discussions, but because they provide better organizational or other functionalities. In many of the cases we examine, it is plausible that manipulating uncertainty of political adversaries is the "main" purpose of these cybersecurity policies, practices, and technologies, especially as they emerged against a backdrop of such intense and violent political competition. But it is not necessary for our argument to establish that manipulating uncertainty is the only reason for a specific action.

The first strategy for minimizing one's own uncertainty in Table 2 is to gather predictive data, and the corresponding first strategy for maximizing an opponent's uncertainty is to keep information secret. The increasing procurement and use of surveillance tools, both targeted and large scale, clearly minimizes uncertainty through (apparent) predictive capability, as it provides governments—specifically security agencies—with more and more detailed intelligence about their targets (which include but are not limited to activists). The secrecy of such intelligence databases, and opacity of the national security apparatus more widely, also means that activists do not know what the government knows about them: they are uncertain as to the extent of digital surveillance in any specific instance. Consequently, secret surveillance tools both minimize government uncertainty and maximize that of their opponents.

On the other side, although some "sousveillance" by activists occurred shortly after 2011 it quickly became less viable in an environment of increasing repression. Nonetheless, leaks around surveillance technologies decreased uncertainty for activists about government intentions and capabilities, as they provided a greater awareness of both specific surveillance capacities and general plans. In this context of increasing online surveillance, some activists used more secure communications technologies, especially VPNs and encrypted messaging, although interviews suggest that there was not widespread adoption of these practices. Others used multiple accounts to hide their political activity from the physical device inspections that became an increasingly common practice for security agencies. These countersurveillance practices increased government uncertainty around who or when political activity would happen, making it harder to pre-emptively act to suppress it. Furthermore, these strategies exhibit a clear dynamic of surveillance/countersurveillance: activists first use new means, such as social media platforms; the state acquires the greater capability to monitor social media; activists expose this capability and move elsewhere; and the state seeks to monitor them again.

Cybersecurity appeared on both sides of this dynamic. Government surveillance was reportedly termed a "Social Networks Security Hazard Monitoring Operation," echoing a wide range of technical and policy measures in cybersecurity. As we have argued elsewhere, companies selling surveillance and intelligence capabilities—including FinFisher and Hacking Team—have embraced descriptions such as "offensive cybersecurity" [60]. These associations appear within a broader view of cybersecurity as protecting "national information space" [3]. Conversely, a "human-centric" view of cybersecurity, closely connected to privacy and fundamental human rights, justified the adoption of countersurveillance practices and technologies by political activists [159]. So both sides were not only manipulating uncertainty, but they were doing so in the name of cybersecurity: the government to protect its information space, and the activists to protect their privacy and individual data security.

The second set of strategies aimed to limit the action space overall, minimizing uncertainty about what your adversary might do, while acting erratically or (apparently) unpredictably, maximizing their uncertainty about what you might do, and creating a dynamic of censorship and creativity. The government, especially from 2016 onwards, greatly increased online censorship, with independent websites and NGO sites explicitly censored for reasons of "terrorism" or "foreign association." However, this censorship was erratic and not systematically enforced, sometimes raising questions about the government's capacity and technological ability, but also due to the encouragement of self-reporting or citizen monitoring. These practices minimized the government's uncertainty by limiting the opportunity for individuals to criticize the government and engage in collective action online, but also increased the uncertainty of activists who did not know when or why they would be blocked. It also mirrors broader offline patterns of arbitrary detention and torture [157].

In response, some activists limited the opportunity for online repression by simply going offline, not taking devices to city center meetings, gatherings, or protests. Others used surprising—not necessarily more secure—means of communication through video game platforms and found creative means of online protest and self-expression, increasing the government's uncertainty about when, where, and how to censor online activity. These strategies were dynamic: as with surveillance/countersurveillance, censorship in one place led activists to migrate somewhere else. However, the chilling effect of overt censorship is much larger than that of unseen surveillance, and so many instead chose to regulate their online speech to avoid censorship.

Cybersecurity was one of several overlapping justifications for censorship, in addition to strengthened counterterrorism and media regulation. The Supreme Cybersecurity Council reportedly played a key role in facilitating online censorship, which was later legitimized by the 2018 Cybercrime Law. This deployment of cybersecurity followed regional patterns, as cybercrime laws in the Gulf states have been used for similar activities, drawing on the permissive position on censorship adopted by the 2010 Arab Convention on Cybercrime [3, 147]. The overlap between cybersecurity and counterterrorism has both a regional and national dimension, with the Saudi Arabia-based cyberterrorism monitoring center "Etidal" supported by regional allies of Egypt, as well as the USA.

In contrast, in terms of responses to censorship, although interviews suggest that some activists viewed practices like leaving devices at home and video-game chat as a form of cybersecurity, creative forms of protest were not connected to cybersecurity in the data reviewed here. This may be because human-centric concepts of cybersecurity focus on privacy rather than freedom of expression more broadly, but it may be due to a lack of available data in comparison to that around government actions. Overall, cybersecurity policies, practices and technologies featured more on the government side of censorship than as a justification for counteractions by activists.

The third set of strategies was the implementation of multiple redundant systems to manage rather than minimize uncertainty, and the use of vagueness and ambiguity to increase opponents' uncertainty. In Section 2, we suggested that although these strategies are conceptually distinct, in practice they support the first two dynamics considered above. The overview of the previous section provided several instances of government actions that involve both redundancy and ambiguity in this way. For example, the introduction of sprawling media, terrorism, and cybercrime laws all aiming to criminalize similar activities – "terrorist" content online—ensures that at least one of the three will be able to suppress almost any undesirable online activity. Conversely, the multiple channels of influence sought by NGOs and rights advocates in response to these laws, from technical advice to individual lobbying, public advocacy and shaping popular opinion, could be seen as a corresponding but ultimately unsuccessful attempt through multiple means to ensure their arguments were heard.

For vagueness and ambiguity, in addition to the characteristics of the cybercrime law noted above, the way the 2012 (and 2014) ICT strategy straddled renewed calls for human rights recognition and repressive national security measures was likely not only due to its attempt to satisfy competing constituencies, but also in order to deliberately remain consistent with a variety of possible policy proposals. We did not identify any strategic use of vagueness and ambiguity by opposition activists relating to cybersecurity in the data reviewed, and represent this with "N/A" in Table 3 below. Consequently, although strategies of redundancy and ambiguity were framed as a question of cybersecurity among other issues, especially by the government, we did not identify a separate dynamic for these strategies.

Overall, our analysis of the emergence of cybersecurity in Egypt from 2011 to 2020 indicates that both government actors and opposition activists sought to manipulate uncertainty: to make the other uncertain about their actions while increasing their certainty about the other's actions. They did so through several distinct strategies, which form distinct but related dynamics of online surveillance/countersurveillance and censorship/creativity. Table 3 provides a summary of the specific policies, practices, and technologies discussed above in relation to strategies of manipulating uncertainty following the layout of Tables 1 and 2, separately for government actors and opposition activists. Our analysis indicates that both sides invoked different interpretations of cybersecurity as part of these strategies, including cybersecurity as national information security and a human-centric, rights-focused version of cybersecurity. However, not all strategies draw an equal connection to cybersecurity (of any form): cybersecurity appears most clearly in all strategies within the first dynamic and predominantly on the government side of the second and third dynamics.

Conclusion

This article has explored the emergence of cybersecurity policies, practices, and technologies in Egypt since the January 25, 2011 revolution. It has been argued that the development of cybersecurity in Egypt has been fundamentally shaped by deep-seated uncertainty about the political process, with a range of actors, especially government security agencies and political activists, deploying different interpretations of cybersecurity as part of technosocial strategies to manipulate uncertainty. In addition to providing extensive empirical data on cybersecurity developments in Egypt over the last decade, this article has made two theoretical contributions. First, it has drawn on and extended scholarship on uncertainty in contentious politics, especially in authoritarian and hybrid regimes, to specify specific strategies of manipulating uncertainty and explore their interaction in dynamics between adversaries. It has been argued that Egyptian politics in this period, with high levels of uncertainty overall, has been characterized by the manipulation of subjective uncertainties to both maintain and challenge dominant power structures. Second, it has shown how new discourses and practices, such as cybersecurity, are assimilated into existing political struggles rather than merely importing their own priorities and structures. This has important implications for cybersecurity studies more widely, as it suggests that political context is essential in understanding state-specific cybersecurity developments. It also highlights international entanglements, as foreign or multinational companies and international NGOs, as well as state relationships, played a key role in cybersecurity developments in Egypt.

The argument here, although located in Egypt, has broader ramifications. It is likely that many other hybrid and authoritarian states, including in the Middle East and North Africa, have treated cybersecurity in similar ways [3, 61, 62]. The use of cybersecurity to manipulate uncertainty may also occur more widely, as what Gunitsky calls "the great convergence" between democracies and authoritarian states leads the former to adopt political practices originally developed in the latter [160]. In democracies such as the USA and the UK, with governments characterized by significant uncertainty over the last few years, the use of cybersecurity discourses and practices to manipulate that uncertainty—e.g., in current debates over the appropriate regulation of end-to-end encryption in the USA—may be increasingly common in the future. But governments are not the only actors whose approach to uncertainty and cybersecurity is still evolving; e.g., the recently founded Amnesty Tech Security Lab seeks to synergize efforts between cybersecurity experts and rights

Table 3: Cybersecurity policies, practices, and technologies in manipulating uncertainty

Dynamic	Actor strategies regarding uncertainty			
	Government		Activist	
	Minimize/manage	Maximize/exploit	Minimize/manage	Maximize/exploit
Surveillance/ countersurveillance	Varied surveillance technologies	Secret databases	Sousveillance, leaks	Encrypted messaging, multiple accounts
Censorship/creativity	Website blocking	Self-reporting	Going offline	Creative online protest (although not linked to cybersecurity)
Redundance/ambiguity (?)	Multiple laws criminalizing content	Vague national strategies/policies	Advocacy for digital rights	N/A

activists and has investigated a range of digital attacks against civil society, including in Egypt.[12]

From the perspective of the study of contentious politics, future research could tease apart the category of opposition activists used in this article, with differences in approach to cybersecurity only gestured toward in the empirical sections. Scholarship of political opposition and protest movements has identified a range of complex relationships between "moderates" and more radical "flanks" [63, 161], and these are likely to manifest in contests over appropriate cybersecurity practices. Future research could also compensate for the weaknesses of a single case study approach by investigating further relevant comparative cases and transnational links at both state and opposition levels, following research trends in contentious politics more broadly [162]. Some starting points for such research were identified, such as the cooperation between several regional states and external allies in countering "cyberterrorism" and procuring surveillance systems, and on the opposite side efforts by transnational civil society to engage in "data activism" and cybersecurity education.

Finally, the argument of this article suggests that the relationship between cybersecurity and uncertainty is more complex than it may first seem. As cybersecurity is oriented toward a range of technological and sociotechnological risks, many cybersecurity practices and technologies seek to accurately calculate those risks, weighing them against other social and economic considerations, and ultimately aiming to lower their likelihood and/or manage them appropriately. Cybersecurity thus seeks to reduce or contain uncertainty. However, the investigation of uncertainty undertaken in this article shows that cybersecurity can also be used in a targeted fashion to manipulate uncertainty for specific groups in contentious politics, relying on secrecy, censorship and ambiguity to increase and exploit uncertainty rather than reduce and contain it. Nonetheless, some forms of uncertainty are crucial for fundamental rights and equitable political systems; indeed, to return to the frame with which we started, uncertainty about outcomes is a productive feature of a healthy democracy. We, therefore, need to recognize how political actors exploit cybersecurity to manipulate uncertainty, while also ensuring that concepts of cybersecurity preserve and protect those forms of uncertainty that we value.

Conflict of interest statement

The authors declare no conflict of interest or specific sources of funding for this research. Financial support for open access publication was generously provided by The Hague Program for Cyber Norms.

Acknowledgments

The authors would like to thank the editors of the special issue, the three anonymous reviewers, the participants of the Hague Program for Cyber Norms Annual Conference, and the TRANSAD Workshop in Barcelona in November 2019, Fatimah Ayad and Nardine Nemr for their feedback on earlier drafts of this article. All remaining errors are ours.

References

1. Shires J. Family resemblance or family argument? Three perspectives of cybersecurity and their interaction. *St Anthonys Int Rev* 2019;**14**:18–36.
2. Hassib B, Alnemr N. Securitizing cyber space in Egypt: the dilemma of cybersecurity and democracy. In Romaniuk SN, Manjikian M (eds.), *Routledge Companion to Global Cyber-Security Strategy*. Routledge, 2021, pp.521–533.
3. Shires J. Ambiguity and appropriation: cybercrime in Egypt and the Gulf. In Broeders, D van den Berg B (eds.), *Governing Cyberspace: Power, Behavior, and Diplomacy*. London: Rowman & Littlefield Publishers, Inc., 2020, pp. 205–26.
4. el-Nawawy M, Khamis S. *Egyptian Revolution 2.0: Political Blogging, Civic Engagement, and Citizen Journalism*. New York, NY: Palgrave Macmillan, 2013.
5. Radsch CC. *Cyberactivism and Citizen Journalism in Egypt: Digital Dissidence and Political Change*. New York: Palgrave Macmillan, 2016.
6. Tilly C. *Contentious Performances*. Cambridge/New York: Cambridge University Press, 2008.
7. Lynch M. *The Arab Uprising: The Unfinished Revolutions of the New Middle East*. New York: PublicAffairs, 2013.
8. Chalcraft J. Egypt's 25 January uprising, hegemonic contestation, and the explosion of the poor. In Gerges FA (ed.), *The New Middle East: Protest and Revolution in the Arab World*. New York: Cambridge University Press, 2013, pp. 155–79.
9. Brownlee J, Masoud T, Reynolds A. *The Arab Spring: Pathways of Repression and Reform*. Oxford/New York: Oxford University Press, 2015.
10. Ketchley N. *Egypt in a Time of Revolution*. Cambridge/New York: Cambridge University Press, 2017.
11. Khiabany G. Technologies of liberation and/or otherwise. *Int J Middle East Stud* 2015;**47**:348–53.
12. Gunitsky S. Corrupting the cyber-commons: social media as a tool of autocratic stability. *Perspect Polit* 2015;**13**:42–54.
13. Emont J. 'Facebook protesters' helped sudan drive out bashir. *Wall Street Journal* April 12, 2019.
14. Bartu P. The new Arab uprisings: how the 2019 trajectory differs from the 2011 legacy? (Part 1). *Al Jazeera Center for Studies*, 5 January 2020. http://studies.aljazeera.net/en/reports/2020/01/arab-uprisings-2019-trajectory-differs-2011-legacy-part-1-200105102004189.html (31 October 2020, date last accessed).
15. Goldsmith J, Wu T. *Who Controls the Internet?: Illusions of a Borderless World*. New York: Oxford University Press, 2008.

[12] https://www.amnesty.org/en/tech/

16. Manjikian MM. From global village to virtual battlespace: the colonizing of the internet and the extension of realpolitik. *Int Stud Q* 2010; **54**:381–401.
17. DeNardis L. *The Global War for Internet Governance*. New Haven, CT: Yale University Press, 2014.
18. Schneier B, Farrell H. *Common-Knowledge Attacks on Democracy.* Harvard University, Berkman Klein Center for Internet and Society, Research Publication No. 2018-7, October 2018.
19. Farrell H, Schneier B. Democracy's dilemma. *Boston Review*, 15 May 2019. http://bostonreview.net/forum-henry-farrell-bruce-schneier-democracys-dilemma (10 January 2021, date last accessed).
20. O'Donnell G, Schmitter PC, Whitehead L. *Transitions from Authoritarian Rule: Tentative Conclusions about Uncertain Democracies*. Baltimore, MD: Johns Hopkins University Press, 1986.
21. Bunce V, Csanádi M. Uncertainty in the transition: post-communism in Hungary. *East Eur Polit Soc* 1993; doi: 10.1177/0888325493007002003.
22. Schedler A. *The Politics of Uncertainty: Sustaining and Subverting Electoral Authoritarianism*. Oxford/New York: OUP, 2013.
23. Lynch M, Freelon D, Aday S. Online clustering, fear and uncertainty in Egypt's transition. *Democratization* 2017;**24**:1159–77.
24. Aradau C, Munster RV. Governing terrorism through risk: taking precautions, (un)knowing the future. *Eur J Int Relat* 2007;**13**:89–115.
25. Daase C, Kessler O. Knowns and unknowns in the 'War on Terror': uncertainty and the political construction of danger. *Secur Dialogue* 2007; **38**:411–34.
26. Goede MD. Beyond risk: premediation and the post-9/11 security imagination. *Secur Dialogue* 2008;**39**:155–76.
27. Kostiner J (ed.). *Middle East Monarchies: The Challenge of Modernity*. Boulder, CO: Lynne Rienner Publishers, 2000.
28. Kandil H. *Soldiers, Spies, and Statesmen: Egypt's Road to Revolt*, London/New York: Verso, 2014.
29. Kandil H. *The Power Triangle: Military, Security, and Politics in Regime Change*. Oxford: Oxford University Press, 2016.
30. Bishara D. *Contesting Authoritarianism: Labor Challenges to the State in Egypt*. Cambridge: Cambridge University Press, 2018.
31. Asad T. Fear and the ruptured state: reflections on Egypt after Mubarak. *Soc Res* 2012;**79**:271–98.
32. Hofstadter R. The paranoid style in American Politics. *Harper's Magazine*, 1 November 1964. https://harpers.org/archive/1964/11/the-paranoid-style-in-american-politics/ (29 June 2020, date last accessed).
33. van Prooijen, J-W, van Lange PAM (eds.). *Power, Politics, and Paranoia: Why People Are Suspicious of Their Leaders*. Cambridge: Cambridge University Press, 2014.
34. Beck U. *Risk Society: Towards a New Modernity*. London: SAGE, 1992.
35. Power M. *The Risk Management of Everything: Rethinking the Politics of Uncertainty*. London: Demos, 2004.
36. Clarke L. *Mission Improbable: Using Fantasy Documents to Tame Disaster*. Chicago, IL: University of Chicago Press, 2001.
37. Greenhill, KM Krause P (eds.). *Coercion: The Power to Hurt in International Politics*. New York, NY: Oxford University Press, 2018.
38. Valeriano B, Jensen B, Maness RC. *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford, NY: Oxford University Press, 2018.
39. Zebrowski C. The nature of resilience. *Resilience* 2013;**1**:159–73.
40. Herrington L, Aldrich R. The future of cyber-resilience in an age of global complexity. *Politics* 2013;**33**:299–310.
41. Dunn Cavelty M, Kaufmann M, Søby Kristensen K. Resilience and (in) security: practices, subjects, temporalities. *Secur Dialogue* 2015; **46**:3–14.
42. Bok S. *Secrets: On the Ethics of Concealment and Revelation*, New York/Toronto, ON: Vintage, 1989.
43. Swire P. *The Declining Half-Life of Secrets and the Future of Signals Intelligence*. Washington, DC: New America Foundation, 2015.
44. Gartzke E, Lindsay JR. Weaving tangled webs: offense, defense, and deception in cyberspace. *Secur Stud* 2015;**24**:316–348.
45. Morris DR. Surprise and terrorism: a conceptual framework. *J Strateg Stud* 2009;**32**:1–27.
46. Nedal D, Nexon D. Trump's 'Madman Theory' isn't strategic unpredictability. It's just crazy. *Foreign Policy*, 18 April 2017. https://foreignpolicy.com/2017/04/18/trumps-madman-theory-isnt-strategic-unpredictability-its-just-crazy/ (29 June 2020, date last accessed).
47. Cornish P. Governing cyberspace through constructive ambiguity. *Survival* 2015;**57**:153–76.
48. Hansen ST. Taking ambiguity seriously: explaining the indeterminacy of the European Union conventional arms export control regime. *Eur J Int Relat* 2016;**22**:192–216.
49. Tilly C. *Regimes and Repertoires*. Chicago, IL: University of Chicago Press, 2006.
50. Hansen L, Nissenbaum H. Digital disaster, cyber security, and the Copenhagen school. *Int Stud Q* 2009;**53**:1155–75.
51. Agrafiotis I, Nurse JRC, Goldsmith M *et al.* A taxonomy of cyber-harms: defining the impacts of cyber-attacks and understanding how they propagate. *J Cybersecurity* 2018;**4**. doi:10.1093/cybsec/tyy006.
52. Barnard-Wills D, Ashenden D. Securing virtual space cyber war, cyber terror, and risk. *Space Cult* 2012;**15**:110–23.
53. Dunn Cavelty M. Breaking the cyber-security dilemma: aligning security needs and removing vulnerabilities. *Sci Eng Ethics* 2014;**20**:701–715.
54. Shires J. Enacting expertise: ritual and risk in cybersecurity. *Polit Gov* 2018;**6**:31–40.
55. Shires J, Smeets M. *Contesting 'Cyber'*. New America Foundation, 2017 [Online]. https://perma.cc/RJ5B-GQXT (10 January 2021, date last accessed).
56. Shires J. Hack-and-leak operations: intrusion and influence in the Gulf. *J Cyber Policy* 2019;**4**:235–56.
57. Stevens T. *Cyber Security and the Politics of Time*. Cambridge: Cambridge University Press, 2015.
58. Shires J. Cyber-noir: cybersecurity and popular culture. *Contemp Secur Policy* 2020;**41**:82–107.
59. Branch J. What's in a name? Metaphors and cybersecurity. *Int Organ* 1–32. undefined/ed, doi:10.1017/S002081832000051X.
60. Shires J. Moral manoeuvres: cybersecurity in Egypt and the Gulf states. D.Phil. Thesis, University of Oxford, Oxford, 2018.
61. Shires J, Hakmeh J. *Is the GCC Cyber Resilient?*. London: Chatham House Royal Institute for International Affairs, 2020.
62. Eldem T. The governance of Turkey's Cyberspace: between cyber security and information security. *Int J Public Adm* 2020;**43**:452–65.
63. della Porta D. On violence and repression: a relational approach (The Government and Opposition/Leonard Schapiro Memorial Lecture, 2013). *Gov Oppos* 2014;**49**:159–87.
64. Davenport C, Moore WH. The Arab spring, winter, and back again? (Re)Introducing the dissent-repression nexus with a twist. *Int Interact* 2012;**38**:704–13.
65. Snow DA, Moss DM. Protest on the fly: toward a theory of spontaneity in the dynamics of protest and social movements. *Am Sociol Rev* 2014; **79**:1122–43.
66. Duyvendak JW, Jasper JM. *Players and Arenas: The Interactive Dynamics of Protest*. Amsterdam University Press, 2015.
67. Duyvendak JW, Jasper JM. *Breaking Down the State: Protestors Engaged*. Amsterdam University Press, 2015.
68. Grimm J, Harders C. Unpacking the effects of repression: the evolution of Islamist repertoires of contention in Egypt after the fall of President Morsi. *Soc Mov Stud* 2018;**17**:1–18.
69. Volpi F, Jasper JM. *Microfoundations of the Arab Uprisings: Mapping Interactions between Regimes and Protesters*. Amsterdam University Press, 2017.
70. Alimardani M, Milan S. The internet as a global/local site of contestation: the case of Iran. In Peeren E, Celikates R, de Kloet J, Poell T (eds.), *Global Cultures of Contestation: Mobility, Sustainability, Aesthetics & Connectivity*, 1st edn. New York, NY: Palgrave Macmillan, 2017.
71. Beraldo D, Milan S. From data politics to the contentious politics of data. *Big Data Soc* 2019. doi:10.1177/2053951719885967.
72. Giandomenico A. Know your enemy: understanding threat actors. *CSO Online*, 27 June 2017. https://www.csoonline.com/article/3203804/know-your-enemy-understanding-threat-actors.html (29 June 2020, date last accessed).

73. Wrightson T. *Advanced Persistent Threat Hacking: The Art and Science of Hacking Any Organization*. New York: McGraw-Hill Education, 2014.
74. Brantly AF (ed.). *The Cyber Deterrence Problem*. London/New York: Rowman & Littlefield Publishers, 2020.
75. Smith GJD. Surveillance, data and embodiment: on the work of being watched. *Body Soc* 2016. doi:10.1177/1357034X15623622.
76. Couldry N, Yu J. Deconstructing datafication's brave new world. *New Media Soc* 2018. doi:10.1177/1461444818775968.
77. Zuboff S. *The Age of Surveillance Capitalism: The Fight for the Future at the New Frontier of Power*. Profile Books, 2019.
78. Mueller ML, Badiei F. Requiem for a dream: on advancing human rights via internet architecture. *Policy Internet* 2019;**11**:61–83.
79. Zalnieriute M, Milan S. Internet architecture and human rights: beyond the human rights gap. *Policy Internet* 2019;**11**:6–15.
80. Lyon D. *The Culture of Surveillance: Watching as a Way of Life*. Cambridge/Medford, MA: Polity Press, 2018.
81. Youmans WL, York JC. Social media and the activist toolkit: user agreements, corporate interests, and the information infrastructure of modern social movements. *J Commun* 2012;**62**:315–29.
82. Bauman Z, Bigo D, Esteves P *et al.* After Snowden: rethinking the impact of surveillance. *Int Polit Sociol* 2014;**8**:121–44.
83. Stoycheff E, Burgess GS, Martucci MC. Online censorship and digital surveillance: the relationship between suppression technologies and democratization across countries. *Inf Commun Soc* 2020;**23**:474–90.
84. Finnemore M, Sikkink K. International norm dynamics and political change. *Int Organ* 1998;**52**:887–917.
85. Mann S. Sousveillance and Cyborglogs: a 30-year empirical voyage through ethical, legal, and policy issues. *Presence Teleoperators Virtual Environ* 2005;**14**:625–46.
86. Hermida A, Hernández-Santaolalla V. Twitter and video activism as tools for counter-surveillance: the case of social protests in Spain. *Inf Commun Soc* 2018;**21**:416–33.
87. Hatakka N. Expose, debunk, ridicule, resist! Networked civic monitoring of populist radical right online action in Finland. *Inf Commun Soc* 2019;**23**:1–16. doi:10.1080/1369118X.2019.1566392.
88. Gürses S, Kundnani A, Van Hoboken J. Crypto and empire: the contradictions of counter-surveillance advocacy. *Media Cult Soc* 2016; **38**:576–90.
89. Dencik L, Hintz A, Cable J. Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data Soc* 2016. doi: 10.1177/2053951716679678.
90. Ataman B, Çoban B. Counter-surveillance and alternative new media in Turkey. *Inf Commun Soc* 2018;**21**:1014–29.
91. Bakir V. 'Veillant panoptic assemblage': mutual watching and resistance to mass surveillance after Snowden. *Media Commun* 2015;**3**:Art. no. 3.
92. The new cyber military-industrial complex. The Globe and Mail. http://www.theglobeandmail.com/opinion/the-new-cyber-military-industrial-complex/article573990/ (9 February 2017, date last accessed).
93. Deibert R. Authoritarianism goes global: cyberspace under siege. *J Democr* 2015;**26**:64–78.
94. Deibert RJ. *Black Code: Inside the Battle for Cyberspace*. Plattsburgh, NY: Signal Books, 2013.
95. Kuo L. TikTok sorry for blocking teenager who disguised Xinjiang video as make-up tutorial. *The Guardian* 28 November 2019.
96. Coleman G. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. London: Verso, 2014.
97. PEN. *Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor*. New York, NY: PEN American Center, 2013. http://www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf (10 January 2021, date last accessed).
98. Penney JW. Internet surveillance, regulation, and chilling effects online: a comparative case study. *Internet Policy Rev* 2017;**6**. https://policyreview.info/articles/analysis/internet-surveillance-regulation-and-chilling-effects-online-comparative-case (28 February 2020, date last accessed).
99. Fathy N. Freedom of expression in the digital age: enhanced or undermined? The case of Egypt. *J Cyber Policy* 2018;**3**:96–115.
100. Grimm JJ, Koehler K, Lust EM *et al. Safer Field Research in the Social Sciences: A Guide to Human and Digital Security in Hostile Environments*. Thousand Oaks: SAGE Publications Ltd, 2020.
101. Privacy International. The President's Men? Inside the Technical Research Department, the secret player in Egypt's intelligence infrastructure, 2016.
102. Karr T. One U.S. corporation's role in Egypt's brutal crackdown. *Huffington Post* 28 January 2011. https://perma.cc/2KR6-D86Q (10 January 2021, date last accessed).
103. Lim M. Clicks, cabs, and coffee houses: social media and oppositional movements in Egypt, 2004–2011. *J Commun* 2012;**62**:231–48.
104. Poell T, Abdulla R, Rieder B *et al.* Protest leadership in the age of social media. *Inf Commun Soc* 2016;**19**:994–1014.
105. Staff Report. Egypt protesters gain ground. *Al-Jazeera*, 9 February 2011. https://www.aljazeera.com/news/middleeast/2011/02/201129103224329921.html (29 June 2020, date last accessed).
106. Azer E, Harindranath G, Zheng Y. Revisiting leadership in information and communication technology (ICT)-enabled activism: a study of Egypt's grassroots human rights groups. *New Media Soc* 2019;**21**:1141–69.
107. Hassanpour N. Media disruption and revolutionary unrest: evidence from Mubarak's quasi-experiment. *Polit Commun* 2014;**31**:1–24.
108. Greenemeier L. How was Egypt's internet access shut off?. *Scientific American* 28 January 2011. https://www.scientificamerican.com/article/egypt-internet-mubarak/ (10 January 2021, date last accessed).
109. Arthur C. Google and Twitter launch service enabling Egyptians to tweet by phone. *The Guardian* 1 February 2011.
110. McVeigh K. British firm offered spying software to Egyptian regime – documents. *The Guardian* 28 April 2011.
111. Raoof R. Egypt: how companies help the government spy on activists. *Global Voices Advocacy* 7 May 2011 https://advox.globalvoices.org/2011/05/07/egypt-how-companies-help-the-government-spy-on-activists/ (29 June 2020, date last accessed).
112. Amin S. Egypt: authorities reveal plans for mass surveillance of social media. *Index on Censorship*, 10 June 2014. https://www.indexoncensorship.org/2014/06/egypt-mass-surveillance/ (29 June 2020, date last accessed).
113. Marquis-Boire M, *Dalek J, McKune S, et al.*. Planet blue coat: mapping global surveillance and censorship tools. *Citizen Lab*, January 2013.
114. MCIT (Egypt). National ICT Strategy 2012-2017: towards a digital society and knowledge-based economy. *MCIT* 2012.
115. MCIT (Egypt), "Publications - Egypt's ICT Strategy 2014 -2017," Ministry of Communications and Information Technology, 2014.. .
116. Schmitter PC, Karl TL. What democracy is. . .and is not. *J Democr* 1991; **2**:75–88.
117. Hassib B. Egypt's counter-terrorism policy post 9/11 and beyond: shrinking civic space. In Romaniuk SN, Mullins S, Ruteere M (eds.). *Terrorism and Civil Society: Post-9/11 Progress and Challenges*. Manchester: Manchester University Press, 2020.
118. Tankel S. *With Us and against Us: How America's Partners Help and Hinder the War on Terror*. New York, NY: Columbia University Press, 2018.
119. Kimball S. After Arab spring, surveillance in Egypt intensifies. *The Intercept*, 9 March 2015. https://theintercept.com/2015/03/09/arab-spring-surveillance-egypt-intensifies/ (29 June 2020, date last accessed).
120. Ahram Online. Egypt to block websites linked to 'terrorism'. *Ahram Online*, 17 February 2015. http://english.ahram.org.eg/NewsContent/1/64/123290/Egypt/Politics-/Egypt-to-block-websites-linked-to-terrorism.aspx (10 January 2021, date last accessed).
121. Staff Report. 3 years for drawing Mickey Mouse ears on Sisi. *Middle East Monitor*, 20 October 2015. https://www.middleeastmonitor.com/20151020-3-years-for-drawing-mickey-mouse-ears-on-sisi/ (29 June 2020, date last accessed).
122. Tesquet O. Amesys: Egyptian trials and tribulations of a French digital arms dealer. *Telerama*, 5 July 2017. https://www.telerama.fr/monde/

amesys-egyptian-trials-and-tribulations-of-a-french-digital-arms-dealer,160452.php (10 January 2021, date last accessed).

123. Frenkel S. U.S. company distances itself from Egyptian surveillance system. *BuzzFeed*, 18 September 2014. https://www.buzzfeednews.com/article/sheerafrenkel/us-company-distances-itself-from-egyptian-surveillance-syste (10 January 2021, date last accessed).

124. Ezzat A. 'You are being watched!' Egypt's mass Internet surveillance. *Mada Masr*, 29 September 2014. https://madamasr.com/en/2014/09/29/opinion/u/you-are-being-watched-egypts-mass-internet-surveillance/ (29 June 2020, date last accessed).

125. Egyptian Supreme Council for Media Regulation. Law No. 180 of 2018 on Regulating the Press, Media, and the Supreme Council for Media Regulation, 2018.

126. AFTE Egypt. Blocked Websites List. *مؤسسة حرية الفكر والتعبير*, 29 June 2020. https://afteegypt.org/en/blocked-websites-list (29 June 2020, date last accessed).

127. Staff Report. Official Report Defends the Website Blockade Decision in Egypt as the Websites Promote Terrorism [Arabic]. *Al-Masry Al-Youm*, 25 May 2017. https://www.almasryalyoum.com/news/details/1139015 (29 June 2020, date last accessed).

128. Trump opens Global Center for Combating Extremist Ideology with Egypt's al-Sissi, Saudi Arabia's Salman. *Washington Post*. http://www.washingtonpost.com/video/politics/trump-opens-global-center-for-combating-extremist-ideology-with-egypts-al-sissi-saudi-arabias-salman/2017/05/21/2875d228-3e4f-11e7-b29f-f40ffced2ddb_video.html (22 May 2019, date last accessed).

129. Al-Sadiq M. Video: Member of Parliament Proposes to Link Facebook Accounts with National Identification Card [Arabic]. *DotMasr*, 16 April 2017. http://www.dotmsr.com/news/196/774928/فيديو-برلماني-يقترح-ربط-الاشتراك-في-فيسبوك-بالرقم-القومي (29 June 2020, date last accessed).

130. Ghaith S. Minister of Communications: we will soon be working on an Egyptian Facebook [Arabic]. *Masrawy*, 12 March 2018. https://www.masrawy.com/news/news_economy/details/2018/3/12/1281050/%D9%88%D8%B2%D9%8A%D8%B1-%D8%A7%D9%84%D8%A7%D8%AA%D8%B5%D8%A7%D9%84%D8%A7%D8%AA-%D9%86%D8%B9%D9%85%D9%84-%D8%B9%D9%84%D9%89-%D8%A5%D9%86%D8%B4%D8%A7%D8%A1-%D9%81%D9%8A%D8%B3-%D8%A8%D9%88%D9%83-%D9%85%D8%B5%D8%B1%D9%8A-%D9%82%D8%B1%D9%8A%D8%A8%D8%A7- (29 June 2020, date last accessed).

131. Staff Report. Facebook accounts with national ID number [Arabic]. *Al-Wafd*, 17 April 2016. https://alwafd.news/حسابات-فيسبوك-بالرقم-القومي 1134325-أخبار-وتقارير (29 June 2020, date last accessed).

132. MM Al-Sisi. Text of the bill sentencing Facebook users without a permit to six-months in prison [Arabic]. *Youm7*, 26 April 2017. https://www.youm7.com/story/2017/4/26/نص-مشروع-قانون-حبس-مستخدمى-فيس-بوك-دون-تصريح/3207466 (29 June 2020, date last accessed).

133. Saker T. MPs suggest Facebook users pay monthly subscription to aid state surveillance. *Egypt Independent*, 16 April 2017. https://www.egyptindependent.com/mps-suggest-facebook-users-pay-monthly-subscription-aid-state-surveillance/ (29 June 2020, date last accessed).

134. AFTE Egypt. Decision from an unknown body: on blocking websites in Egypt. 4 June 2017. https://afteegypt.org/en/right_to_know-2/publicationsright_to_know-right_to_know-2/2017/06/04/13069-afteegypt.html (29 June 2020, date last accessed).

135. Greenberg A. Encryption app 'signal' is fighting censorship with a clever workaround. *Wired*, 21 December 2016.

136. Marlinspike M. A letter from Amazon. *Signal Messenger*, 1 May 2018. https://signal.org/ (29 June 2020, date last accessed).

137. Scott-Railton J, Marczak B, Raoof R *et al.* Nile Phish: large scale phishing campaign targeting Egyptian civil society. *Citizen Lab*, 2 February 2017.

138. Raoof R. Two-step verification in Egypt: strength or weakness for online security?. *Global Voices Advocacy*, 7 April 2016. https://advox.globalvoices.org/2016/04/07/two-step-verification-in-egypt-strength-or-weakness-for-online-security/ (29 June 2020, date last accessed).

139. Al-Bermawy A. Details on hacking Ola Shohba's account and Vodafone responds [Arabic]. *Tahrir News*, 15 July 2017. https://www.tahrirnews.com/Story/806209/%D8%AA%D9%81%D8%A7%D8%B5%D9%8A%D9%84-%D8%A7%D8%AE%D8%AA%D8%B1%D8%A7%D9%82-%D8%AD%D8%B3%D8%A7%D8%A8%D8%A7%D8%AA-%D8%B9%D9%84%D8%A7-%D8%B4%D9%87%D8%A8%D8%A9-%D9%88-%D9%81%D9%88%D8%AF%D8%A7%D9%81%D9%88%D9%86-%D8%AA%D8%B1%D8%AF/%D9%85%D8%B5%D8%B1 (29 June 2020, date last accessed).

140. Staff Report. German-made FinSpy spyware found in Egypt, and Mac and Linux versions revealed. *Amnesty International*, **25** September 2020. https://perma.cc/WG28-RH4L (27 September 2020, date last accessed).

141. Abu Omar A. IMF deal to keep party going for world's carry-trade darling. *Bloomberg.com*, 26 June 2019.

142. Staff Report. Sources: officials delayed survey results showing Egyptians face highest poverty rate since 2000. *Mada Masr*, 30 July 2019. https://perma.cc/D4ZC-YA7D (10 January 2021, date last accessed).

143. Hamama M, El Sharnoubi O. Is the government building a parallel bureaucracy?. *Mada Masr*, 16 May 2019. https://perma.cc/PT5Z-TWVC (10 January 2021, date last accessed).

144. Deknatel F. Egypt's Sisi is repeating Mubarak's economic mistakes, to the IMF's applause. *World Politics Review*, 21 May 2019. https://perma.cc/RD2H-TQH5 (10 January 2021, date last accessed).

145. Davidson J, Tolba A. Egypt's Sisi wins 97 percent in election with no real opposition. *Reuters*, 2 April 2018.

146. EIPR, SITC Egypt, and AFTE Egypt. Anti-technology [Arabic]. Cairo, June 2016.

147. Hakmeh J. Cybercrime and the digital economy in the GCC countries. Chatham House - The Royal Institute for International Affairs, June 2017.

148. Staff Report. TIMEP Brief: 2019 Constitutional Amendments. *Tahrir Institute for Middle East Policy*, 17 April 2019. https://timep.org/reports-briefings/timep-brief-2019-constitutional-amendments/ (29 June 2020, date last accessed).

149. Supreme Cybersecurity Council. *National Cybersecurity Strategy 2017-2021*. Arab Republic of Egypt, 2018.

150. Gleicher N. Removing coordinated inauthentic behavior in UAE, Egypt and Saudi Arabia. *About Facebook*, 1 August 2019. https://about.fb.com/news/2019/08/cib-uae-egypt-saudi-arabia/ (29 June 2020, date last accessed).

151. DFRLab. Facebook disabled assets linked to Egypt and UAE-based firms. *Medium*, 14 August 2019. https://medium.com/dfrlab/facebook-disabled-assets-linked-to-egypt-and-uae-based-firms-a232d9effc32 (29 June 2020, date last accessed).

152. Twitter Safety. Disclosing new data to our archive of information operations. *Twitter Safety*, 20 September 2019. https://blog.twitter.com/en_us/topics/company/2019/info-ops-disclosure-data-september-2019.html (29 June 2020, date last accessed).

153. Gleicher N. Removing coordinated inauthentic behavior in UAE, Nigeria, Indonesia and Egypt. *About Facebook*, 30 October 2019. https://about.fb.com/news/2019/10/removing-coordinated-inauthentic-behavior-in-uae-nigeria-indonesia-and-egypt/ (29 June 2020, date last accessed).

154. MEMO. Egypt contractor accuses army of squandering public funds amid austerity. *Middle East Monitor*, 4 September 2019. https://www.middleeastmonitor.com/20190904-egypt-contractor-accuses-army-of-squandering-public-funds-amid-austerity/ (29 June 2020, date last accessed).

155. Malsin J, El-Fekki A. Egypt curbs online dissent with street searches: 'he asked to see my phone'. *Wall Street Journal*, 7 October 2019.

156. Netblocks. Facebook Messenger, social media and news sites disrupted in Egypt amid protests. *NetBlocks*, 22 September 2019. https://netblocks.org/reports/facebook-messenger-social-media-and-news-sites-dis

rupted-in-egypt-amid-protests-eA1Jd7Bp (29 June 2020, date last accessed).

157. Guerin O. The shadow over Egypt. *BBC News*, 23 February 2018. https://www.bbc.co.uk/news/resources/idt-sh/shadow_over_egypt (10 January 2021, date last accessed).

158. OTF Information Controls Fellow. Digital authoritarianism in Egypt: digital expression arrests 2011-2019. *Open Technology Fund*, October 2019.

159. Deibert RJ. Toward a human-centric approach to cybersecurity. *Ethics Int Aff* 2018;**32**:411–24.

160. Gunitsky S. The great online convergence: digital authoritarianism comes to democracies. *War on the Rocks*, 19 February 2020. https://warontherocks.com/2020/02/the-great-online-convergence-digital-authoritarianism-comes-to-democracies/ (20 February 2020, date last accessed).

161. Ellefsen R. Deepening the explanation of radical flank effects: tracing contingent outcomes of destructive capacity. *Qual Sociol* 2018; **41**:111–33.

162. Porta, DD Tarrow S (eds.). *Transnational Protest and Global Activism*. Lanham, MD: Rowman & Littlefield Publishers, 2004.