TACTICS INSTITUTE
For Security & Counter Terrorism

Analyzing the UAE-Chinese Cyber Security Alliance

Erasmus University College

ASU Arizona State University

May 2022

The Tactics Institute for Security and Counter-Terrorism is an independent think tank that popularises security discourse, bridging the worlds of academia, policymaking, civic advocacy, and security. We focus on the intersection of home affairs and national security, combining practitioners' experience with a policy development perspective. At Tactics Institute, we identify emerging security trends and bring them to the fore for public discussion and reflection. We do this always with a view to discrediting political violence and enhancing the resilience of open and pluralistic democracies.

Contents

PREFACE 4
ALEXANDRU GEORGESCU

I. Cyber Democracy 9
LORA PITMAN

II. Elite Hacking and Corporate Espionage: Comparing the Chinese and the UAE Authoritarian Modus Operandi of Using Proxies in Cyberspace 19
METODI HADJI-JANEV

III. State Surveillance under Human Rights Law in the China-UAE Cyber Security Alliance 33
ALEXANDROS SARRIS

About the Authors 52

PREFACE

ALEXANDRU GEORGESCU

The following report offers a significant contribution to our understanding of the evolving subject of cyber governance and cyber security. The title is deceptive in that the report itself goes far beyond the descriptive and veers strongly into the prescriptive, where a significant contribution is made especially from the perspective of the reconciliation between cyber security and human rights through a proposal on human-centric security.

Cyber security is not just a generational buzzword, but also a universal concern that impacts areas from privacy to safety, from crime to security from rival powers to the security of critical infrastructures that are global in scope. The development of the Internet, the digitization of all walks of life, and the digitalization of our entire data sphere are enabling new capabilities, such as cyber democracy, new efficiencies in economic processes and new horizons in the transborder and transcultural exchange of knowledge and ideas. At the same time, new advances such as 5G communications, the Internet-of-Things and technologies such as quantum computing, blockchain and artificial intelligence promise a qualitative leap forward for the domain, making possible new capabilities, new applications, new products and services, and new dimensions of interaction. Sooner rather than later, all critical infrastructures on which we rely will be governed and connected (sectorally and geographically) through a cyberspace medium enabling command, control, coordination and data-gathering functions. It has been termed a revolution in commerce and communications, and the pandemic has shown it to be a revolution in education, work and public administration. But it is also a continuous transformation that far outstrips our capacity to anticipate systemic issues, to keep up and to address the risks, vulnerabilities and threats that it engenders. The goal is not only to prevent human losses, material damage and loss of confidence in authorities and institutions but to do so in a way that preserves and even enhances cherished freedoms and human rights.

This report is a timely and substantial addition to the ongoing discussions, focusing in its analysis on the UAE and on China as two models for development of an authoritarian-leaning mode of cyber security governance that may contrast with the West's professed values and rhetoric but are the product of incentives, trends and pressures that the West itself is subject to. Therefore, the two countries may be seen as mirrors of what the main Western powers and what smaller liberal countries may choose to implement, unintentionally walking in the footsteps of China and the UAE respectively, if the issues of human rights and freedom are not kept at the forefront of policy- and decision-makers' concerns.

The report is made up of three distinct sections, each with a different author, with a different style and voice. If I am to recommend the report in the briefest possible terms, I would call it "eminently quotable", in addition to having exquisitely

structured treatments of the subject matter that could have belonged in a monograph. The descriptions of the three chapters will be peppered with choice quotes from the authors themselves, often from different sections of the report which feed into a compelling narrative of standing on the threshold of great changes which demand care in the preservation and promotion of human-centric security.

The first chapter, simply titled "Cyber Democracy", analyses the tension between the expectations of the cyber realm as a medium of exchange for ideas ultimately resulting in more inclusive, responsive and deliberative forms of governance, and the reality of its implementation, which has seen a striking quality of favouring autocratic forms of socio-political control and centralization. States may "control the information flows and use intrusive methods and technologies against peer competitors and domestic opposition, while uniquely exploiting the openness of democracies". The use of state proxies in cyber space "provides authoritarian regimes with an asymmetric advantage at the expense of complex challenges to aspirations and efforts for liberal cyber governance". In a description that reoccurs throughout the report, both states have leveraged their particular strengths to address their weak areas in building organizations, instruments and partnerships for a cyber security regime that strays from what could be construed as legitimate into an area of potential political and social repression. The structures being built are not employed by way of exception or as a response to force majeure but as an ordinary addition to the apparatus of governance providing an additional measure of control for authorities without safeguards for arbitrariness, exclusion and illegitimacy.

China, with its significant resources and internal capacity, has built national champions that perform the exact functions of Western equivalents but are shielded from competition by significant barriers to entry, forming its own digital ecosystem that can produce viable competitors for global markets, but which is also used to produce hitherto unknown levels of information gathering and control over its population. Paraphrasing the words of American scientist James C. Scott, China is using digital technology to increase the legibility of Chinese society, in order to detect deviations from ideological orthodoxy and to manage its dynamic online space in order to ward off disharmony and subversion by enemies, both foreign and domestic.

The UAE has leveraged its significant resources and partnerships abroad to accrue the best tools and the best expertise in order to construct a cyber security apparatus that is also used to silence activists and to control speech.

The two are linked not by the commonality of needs between autocracies with nevertheless different political systems, but also by a web of exchanges and partnerships that disseminate the tools for reducing cyber freedoms and distancing reality from the ideal of cyber democracy as a "two-way communication between the people in the country, on the one hand, and between the people and the government, on the other". It is mentioned that "these tools are used to surveil populations for signs of dissent and to detect political opposition. They are also used to undermine adversaries abroad, extending states' reach internationally" and that "China is the largest exporter of such tools".

The second chapter represents the largest contribution to the subject of the UAE-China

cyber security alliance and is titled "Elite hacking and Corporate Espionage: Comparing the Chinese and the UAE authoritarian modus operandi of using proxies in cyberspace". Like the previous chapter, it is descriptively rich and well researched, with a wealth of bibliographical sources.

Authoritarian states especially took to the cyber realm as their deficiencies in conventional military power and technological competitiveness required a new equalizing dimension, which was found in the technological and policy "voids" left by "the convergence between the cyber and physical space".

A few key ideas stand out from this chapter, which emphasize fine distinctions that have important policy and regulatory implications. The first is a very strong criticism of "the privatization of national security [..] this liberal driven logic has incentivized the majority of Western states and their allies to outsource and become highly dependent on private corporations for logistics, and research and development." This creates a host of problems, including moral hazard on the part of private company employees with access to sensitive data or to the private data of citizens. It is important to remember that actors such as Edward Snowden accessed sensitive information which was released to the public while working for a private contractor to the state in intelligence matters. Abuses have frequently appeared in the media, sometimes under fanciful monikers such as LoveINT, where individuals lacking the filters, training, indoctrination and socialization of government entities such as the military end up to a much greater degree as risks for spying on current or former spouses and partners. The chapter focuses especially on how "building on this accessibility and anonymity, authoritarian regimes have proved capable of utilizing complex and hardly identifiable practices immersed under liberal virtues, such as the open market, outsourcing, knowledge and technology transfer, and open access to information to hide their activities and ambitions". The system itself is eminently exploitable by actors, within or without, seeking outcomes which are incompatible with Western values and norms and leveraging, especially in the case of internal elites, "an unmatched understanding of the current cyber, espionage, and national security risk and regulatory landscape".

Particular care is given throughout the chapter to emphasize the different types of proxies and their evolution in time, as not only technology develops, but also the state's capacity to finetune, direct or delegate actions to proxies, whether they are "patriotic hackers", cyber militias, internal elite units or hired private companies and even Western experts, sometimes with a limited understanding of what they are enabling – "transnational digital authoritarianism is particularly subtle, pernicious and low-cost since it circumvents issues of national sovereignty and does not require travel, or direct government involvement." Particular care is given to differentiate China and the UAE, the latter having an especial reliance on Western experts working for proxies which are "state-sponsored but are not officially deemed to be working under regular state formations. Although officially working independently of the state, this lucrative partnership provides these cyber individuals, groups, or formations with the advantage of extensive resources, including time and money to achieve persistence, allowing the

capability of achieving global reach using advanced tradecraft."

The challenges posed by distributed capabilities across multiple stakeholders with cyber security impact (such as government units, military units, private companies, civil society or organized crime groups) lead to a complex topology of authoritarian cyber security structures, the solutions to which are quite tricky to design and implement. Potential approaches include limiting the export of software with illegitimate use and banning employment contracts between Western experts and companies in states identified as digital authoritarians.

The final chapter, titled "State Surveillance under Human Rights Law in China-UAE Cyber Security Alliance", makes the largest prescriptive contribution to the report, by dissecting the myriad way in which human rights can be affected by digital authoritarians cloaking their actions in pernicious or imprecise language – loaded terms such as "war" and an "arms race" are frequently inappropriate to describe what is going on and what is often reported in the media as examples of "cyber wars" do not entail violence and should more appropriately be referred to as instances of "cyber espionage". Acts of espionage are usually governed by different legislation than acts of warfare.

The use of loaded and imprecise language, as well as the deliberate confusion between cyber security and cyber surveillance, which are often at loggerheads, since the latter is often promoted and facilitated at the expense of the former, have had significant and far-reaching consequences – "many governments are using vague internal and external threats as arguments to justify ever-greater investments in cyber arms and mass surveillance schemes, and ever greater governmental control of the Internet and their citizens [...] Such measures often pose threats to civil liberties, yet they tend to lack judicial oversight as well as public data on which to judge their effectiveness (often because of claims that disclosure would impact on security efforts)."

The chapter reaches a climax in its description of a human-centric or citizen-centric security policy, which enshrines two crucial components – the right to privacy and the right to free speech. These are two areas already beset by moral hazard and (sometimes willful) imprecision in definitions and terms. On the one hand, the cooperation between companies and governments often leads to inappropriate transfers of data without respecting appropriate safeguards. On the other hand, there has been a tendency to lump things such as hacktivism with criminality and terrorism, even when the politically motivated hackers' actions could be construed as legitimate speech – "Hacktivists are often lumped together with cyber criminals in cyber security strategies, but it is important to distinguish between crimes and actions which can be more accurately defined as an attempt to protest and effect change."

What is proposed is a globally distributed multistakeholder model for Internet governance that limits the capacity for abuse by introducing checks and balances through actors beyond the reach of a single political leadership unit – "the establishment of networks of governance actors and institutions, both domestically and internationally, who are linked in multiple ways and have a crucial stake in supporting and collaborating with each other." States play a vital role, not just as an extension of

their institutional and security prerogatives, but also because they "all too often engage in deliberate manipulation of security weaknesses and threats to their own ends", which is why "this approach also requires a strong commitment to mutual restraint as envisioned under international human rights law."

The report "Analyzing the UAE-Chinese Cyber Security Alliance" delivers on the comparative analysis but, on the way, it generates a comprehensive analysis of the intersection between cyber transformations and Western political values and freedoms. Its short length and deep content should mark it as a document of reference in the study of the clash between authoritarian temptation and the basis of human rights. Beyond the deliberate and planned authoritarianism of China and the UAE, the report sounds the alarm on the gradual enshrinement in the West of a "negative conception of security [which] has led to policies and practices which disempower the people they seek to serve". The interconnectedness of all actors, domains and perspectives through the metadomain of cyber space has produced a new level of complexity, felt not just through cyber warfare, espionage and crime, but also through risks, vulnerabilities and threats to freedoms, rights and the underlying principles of Western-inspired political systems.

I. CYBER DEMOCRACY

Lora Pitman

For years, the question, "what constitutes a working democracy?" has interested the academic community. Diamond and Morlino [1] respond to this question and emphasize five conditions determining how successful a democracy is: 'freedom, the rule of law, vertical accountability, responsiveness and equality'. With this in mind, cyber democracy should be understood as a never-ending strive to achieve - through computer and information technology - a high level of freedom and lawfulness, including the accountability of the ruling elite, matching public needs with policy, and the equal treatment of all participating members of the community. Democracy, and specifically cyber democracy, should be viewed as an expression of these aforementioned goals through the free production and dissemination of knowledge online.[2]

In the following sections, each component's role and meaning in relation to the concept of cyber democracy will be discussed. Following this, the components will be assessed in the context of the current cybersecurity policies of China and the United Arab Emirates (UAE) respectively. Lastly, the implications of the China-UAE cyber alliance for the development of cyber democracies worldwide will be discussed.

The concept of freedom encompasses political, civil, economic, social and cultural rights for citizens.[3] In a cyber-democracy, such rights should be provided, maintained, and defended through the free production and dissemination of knowledge, as mentioned above. In practice, in a digital environment, citizens would be able to benefit from obtaining information on political parties, their platforms, their ideologies and their agenda from the Internet. Moreover, they would be able to access accurate and trustworthy information about the current government, the services it offers to citizens, its actions, and its plans for the future.

E-voting is one of the goals of cyber democracy, but there are still various obstacles that make states hesitant to adopt it. Lauer [4] cites concerns among cybersecurity experts around election security and the possible interference by foreign powers. In 2014 CyberBerkut, a group of Russian hacktivists, targeted the Ukrainian Central Election Commission

[1] Larry Diamond and Leonardo Morlino, "The Quality of Democracy: An Overview", vol. 15, no. 4, *Journal of Democracy*, 2004, pp. 21, https://doi.org/10.1353/jod.2004.0060.
[2] David F. J. Campbell and Elias G. Carayannis, "Overview of Cyber-Democracy", in *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, ed. Elias G. Carayannis, David F. J. Campbell, and Marios Panagiotis Efthymiopoulos (Cham: Springer International Publishing, 2018), 323–26, https://doi.org/10.1007/978-3-319-09069-6_72.
[3] United Nations general Assembly, "Universal Declaration of Human Rights (UDHR)" (1948), https://www.ohchr.org/EN/Issues/ESCR/Pages/ESCRIndex.aspx.
[4] Thomas W. Lauer, "The Risk of E-Voting", vol. 2, no.3, *Electronic Journal of E-Government*, 2004, pp. 177–86, https://issuu.com/academic-conferences.org/docs/ejeg-volume2-issue3-article34.

bringing its network down,[5] nearly leading to the announcement of a false winner. Despite this, companies continue to develop the software necessary for e-voting, and states continue to adopt it at amazing speed. Evidence suggests electronic voting offers greater security and transparency, increasing participation and trust in the electoral process. In Brazil, research has shown that the adoption of electronic voting increased voter accessibility to the ballot and led to greater de facto enfranchisement of mainly low-income voters – leading, as a result, to increased government spending on healthcare services.[6] Similarly in India, research has shown that the use of electronic voting machines to replace paper ballots has reduced electoral fraud.[7]

Every democracy should consider the rule of law as a superior norm that treats all citizens equally. Often, the right to online privacy clashes with the desire to create a safe and secure environment, of which algorithms are seen as a key component. Algorithms are aimed at optimizing processes. They secure communication across the public channels of the Internet, providing an easy way to hide information from prying eyes, allowing private communications, online banking, and digital shopping to take place securely online. Still, experts worry that governments and corporations have too much market control and power over algorithmic use; that algorithms perpetuate bias, cut creativity, reduce choices, and could worsen economic inequality. In addition, such practices are shown to be negatively biased toward certain groups of the population.[8]

Police are increasingly using data-driven algorithms to predict crime. However, for many, this system targets and justifies racial profiling. Arrest data biases predictive tools and leads to a greater police presence and a greater number of arrests in certain neighborhoods.[9] Evidence shows that these tactics are applied predominantly in poor and minority communities.[10] Predictive algorithms are often built upon information collected through various forms of unauthorized surveillance, which violates the right to privacy; moreover, the data is used in an obscure, unclear, and almost secretive manner to construct a supposedly fair algorithm.[11] Nick Lally[12] concludes that 'modularity opens predictive policing up to

[5] Cyber Law ToolKit, "Ukrainian parliamentary election interference (2014)", n.d., https://cyberlaw.ccdcoe.org/wiki/Ukrainian_parliamentary_election_interference_(2014).

[6] Thomas Fujiwara, "Voting Technology, Political Responsiveness, and Infant Health: Evidence From Brazil", vol. 83, no. 2, *Econometrica*, 2015, pp. 423–464, https://www.princeton.edu/~fujiwara/papers/elecvote_site.pdf.

[7] Shamika Ravi, Sisir Debnath, and Mudit Kapoor, "The Impact of Electronic Voting Machines on Electoral Frauds, Democracy, and Development", *Brookings Instituion*, https://www.brookings.edu/wp-content/uploads/2016/10/evm_march2017.pdf.

[8] Kristian Lum and William Isaac, "To Predict and Serve?," *Significance* 13, no. 5 (2016): 14–19, https://doi.org/10.1111/j.1740-9713.2016.00960.x.

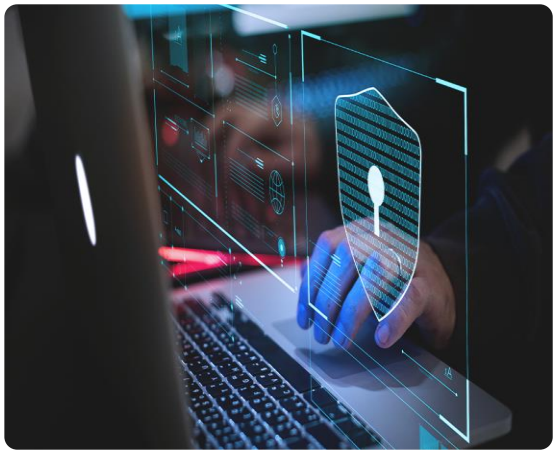
[9] Andrew G. Ferguson, "Policing Predictive Policing", Washington University Law Review, Vol.94, No.5 (2017): 1109-1189. Available at: https://openscholarship.wustl.edu/law_lawreview/vol94/iss5/5.

[10] Vidushi Marda and Shivangi Narayan, "Data in New Delhi's Predictive Policing System," in *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, FAT* '20 (New York, NY, USA: Association for Computing Machinery, 2020), 317–24, https://doi.org/10.1145/3351095.3372865; Sarah Brayne, "Big Data Surveillance: The Case of Policing," *American Sociological Review* 82, no. 5 (October 1, 2017): 977–1008, https://doi.org/10.1177/0003122417725865.

[11] Kiana Alikhademi et al., "A Review of Predictive Policing from the Perspective of Fairness," *Artificial Intelligence and Law*, April 15, 2021, https://doi.org/10.1007/s10506-021-09286-4.

[12] Nick Lally, "'It Makes Almost No Difference Which Algorithm You Use': On the Modularity of Predictive Policing," *Urban Geography*, July 2, 2021, 15, https://doi.org/10.1080/02723638.2021.1949142.

untold abuses, as numerous data and functions can be plugged in and mixed together for questionable purposes.' These purposes can be used by governments for political causes, frequently without accountability – a core tenet of democracy and cyber democracy.



Accountability or more accurately, vertical accountability, is also among the most important components of every democracy. It refers to the accountability of a government to its citizens, alongside the necessary constraints placed on a government's use of political power. In a cyber-capacity, this would include the communication that those in power need to establish with their citizenry in order to promote trust and reliability. Naturally, in non-democracies, the issue of accountability is blurred. However, this does not mean that in non-democracies there are no efforts to maintain some public satisfaction with the government. While there may be an absence of an electoral process, states can still demonstrate a strong commitment to good governance. While legitimacy is not reaped from popular representation and democratic accountability, such regimes still require the acquiescence of their citizenry. In this case, the role of propaganda replaces the requirement of accountability in the form of the dissemination of arguments, accurate information, and fact-based policies. The online environment is, therefore, an important medium for influencing public opinion, especially in non-democracies, within which an alternative to state-supported sources of information and knowledge may be limited by those in power.

Equality is the component of democracy and cyber democracy with which most countries seem to be struggling. It corresponds with the component of freedom, but it considers the individual's status as part of the community, in comparison with other core individual rights and responsibilities. While in most democracies each citizen over a certain age is eligible to vote in elections (and be elected), there are still some exceptions that are established by law that prevent certain citizens from being able to do so. In non-democracies, political equality does not have the same value, as citizens have a minimal, if any, role in the country's governance. Equality in these countries and even in certain democracies carries greater meaning when the issue of privilege is considered.

While the Internet was expected to be the 'great equalizer', bringing equality across class, gender, racial and ethnic lines; some scholars argue that not only did it not compensate for these differences, but it

reinforced them or made them worse.[13] [14] In terms of equality, when it comes to civic engagement and education, democracies are falling short of meeting the desired goal, as people who participate in online civic life tend to be richer and better educated. [15] Additionally, a global digital divide exists in different parts of the world in regard to online access.[16] Data from the International Telecommunications Union [17] show that 87% of the people in developed countries have access to the Internet, compared to 47% of the people in developing countries, and only 19% for the least developed ones. For non-democracies, the same observation applies, with government-imposed restrictions over Internet access further impeding their ability to be contributing members of society.

Cyber democracy and China's cybersecurity strategy

The element of freedom in the concept of cyber democracy has a limited role in China because of its regime type. The desired two-way communication between the citizenry on the one hand, and between the people and the government on the other, is replaced with a carefully designed approach by the state when it comes to more sensitive topics. The online content that Chinese cyber citizens are allowed to view is curated to a large extent by the regime. Facebook, Google, Twitter, Snapchat, DropBox, Reddit and others are all banned from being accessed, and Apple is subject to strict rules about the apps it offers.[18] Some of the social media apps which are permitted resemble the Western equivalents of these means of communication. However, they appear to be allowed by the state for specific reasons, namely as a form of surveillance and social control.[19]

Contrary to common perceptions and some efforts by the state to silence opposition to the regime, and to views critical of it, studies show that the relationship between the Chinese government and social media is more complex. Qin, Strömberg, and Wu[20] explain this relationship in the following way: While there are a lot of voices speaking against the system and its methods, there are only a handful that are capable of provoking any meaningful change that will affect the regime negatively, and those are

[13] Jen Schradie, "The Great Equalizer Reproduces Inequality: How the Digital Divide Is a Class Power Divide", in *Rethinking Class and Social Difference*, ed. Barry Eidlin and Michael A. McCarthy, vol. 37, Political Power and Social Theory (Emerald Publishing Limited, 2020), 81–101, https://doi.org/10.1108/S0198-871920200000037005.

[14] Petter Bae Brandtzaeg, "Facebook Is No 'Great Equalizer': A Big Data Approach to Gender Differences in Civic Engagement across Countries", vol. 35, no. 1, *Social Science Computer Review* 35, 2017, pp. 103–25, https://doi.org/10.1177/0894439315605806.

[15] Aliya Sternstein, "Wealthy, well-educated more likely to engage in online civic activities", Nextgov, 1 September 2009, https://www.nextgov.com/about/?oref=ng-nav.

[16] Monica Anderson and Madhumitha Kumar, "DIGITAL DIVIDE Persists Even as Lower-income AMERICANS Make Gains in Tech Adoption", PEW RESEARCH Center, May 2019, HTTPS://www.PEWRESEARCH.ORG/ fact-tank/2019/05/07/DIGITAL-DIVIDE-PERSISTS-EVEN-as-LOWER-income-AMERICANS-MAKE-GAINS-in- TECH-ADOPTION/.

[17] International Telecommunications Union, "Measuring Digital Development: Facts and Figures", 2019, https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf.

[18] Paige Leskin, "Here Are All the Major US Tech Companies Blocked behind China's 'Great Firewall,'" Business Insider, October 10, 2019, https://www.businessinsider.com/major-us-tech-companies-blocked-from-operating-in-china-2019-5.

[19] Baohua Zhou, "Fear of Missing out, Feeling of Acceleration, and Being Permanently Online: A Survey Study of University Students' Use of Mobile Apps in China", vol. 12, no.1, *Chinese Journal of Communication*, 2019, pp. 66–83, https://doi.org/10.1080/17544750.2018.1523803.

[20] Bei Qin, David Strömberg, and Yanhui Wu, "Why Does China Allow Freer Social Media? Protests versus Surveillance and Propaganda", vol. 31, no. 1, *Journal of Economic Perspectives* 31, no. 1, 2017, pp. 117–40, https://doi.org/10.1257/jep.31.1.117.

the ones being censored.[21] At the same time, allowing for some free speech on social media enables the government to stay informed about public opinion and the potential for collective action.[22] There is also another characteristic that makes China's approach to cyberspace unique. As a communist state, China is expected to apply censorship through its own channels. However, this is not the only tool it is using to gather information. In the case of Beijing, the tactic of surveillance capitalism [23] employed by the private sector benefits the government, as the former sell users' data to the latter, thus supporting their mass surveillance campaigns and social control efforts.[24] Interestingly, one study found that this form of social control is not exercised as direct propaganda, but rather as a public distraction when controversial topics are discussed in the cyber realm. [25] Despite these setbacks, Internet users in China have a powerful weapon in the fight for one of cyber democracy's most important elements: online freedom. VPNs are frequently used to circumvent the limitations imposed by the regime. That said, another element of cyber democracies – lawfulness – seems to contradict the right of freedom to access information, as in January 2017, China made it illegal for service providers to sell VPNs to customers and even sentenced a number of them to jail time.[26] There are other examples of laws intended to suppress free speech and access to information as well, in cases in which they 'expose state secrets and endanger the country',[27] regardless of the officially proclaimed right in Article 35 of China's constitution which declares the right to free speech and a free press.[28] In this case, the laws are indeed followed, but if they oppose another part of the cyber democracy concept, this element of lawfulness loses its meaning.

Since Chinese citizens are not voting to elect their government officials, the aspect of accountability of the ruling elite also has a limited role. Regardless, there are some actions taken by the government to announce and justify their policies and decisions. For instance, the Chinese

[21] Gary King, Jennifer Pan, and Margaret E. Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression", *American Political Science Review* 107, no. 2 (May 2013): 326–43, https://doi.org/10.1017/S0003055413000014.
[22] Qin, Strömberg, and Wu, "Why Does China Allow Freer Social Media?"
[23] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Hachette, 2019).
[24] Rui Hou, "Neoliberal Governance or Digitalized Autocracy? The Rising Market for Online Opinion Surveillance in China," *Surveillance & Society* 15, no. 3/4 (August 9, 2017): 418–24, https://doi.org/10.24908/ss.v15i3/4.6610.
[25] Gary King, Jennifer Pan, and Margaret E. Roberts, "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument," *American Political Science Review* 111, no. 3 (August 2017): 484–501, https://doi.org/10.1017/S0003055417000144.
[26] Sonali Chandel et al., "The Golden Shield Project of China: A Decade Later—An In-Depth Study of the Great Firewall", 2019, 119, https://doi.org/10.1109/CyberC.2019.00027.
[27] Beina Xu and Eleanor Albert, "Media Censorship in China", Council on Foreign Relations, 17 February 2017, https://www.cfr.org/backgrounder/media-censorship-china.
[28] The National People's Congress of the People's Republic of China, "Constitution of the People's Republic of China", 2004, http://www.npc.gov.cn/zgrdw/englishnpc/Constitution/2007-11/15/content_1372964.htm.

Communist Party (CCP) coined the term 'whole process of people's democracy'[29] – an alternative to the Western understanding of democracy. There are multiple documents testifying to Beijing's efforts to popularize and defend the term, both domestically and internationally. In December 2021 on the website of the *Global Times*, published under the guidance of the CCP, was extensive material with a Q&A regarding the newly introduced concept. In theory, it incorporates all of the elements of democracy, but the practical expression of them is restricted, if not entirely absent. The source emphasizes that government units are 'accountable to the people and subject to public oversight', that they 'reach the greatest common ground based on the wishes and needs of the whole of society', and that they apply 'the principle of equality of citizens, regions and ethnic groups'.[30] In sharp contrast with these statements are the many cases of silenced and/or imprisoned critics of the regime and people making accusations against its officials,[31] alongside human rights activists.[32] [33]

In terms of equality, after many years of mistreatment of women and of families giving preference to sons over daughters, [34] gender equality appears to be one of the goals of modern China as it aims to continue its economic growth. [35] That said, some context must be added. Chinese women experience high domestic abuse rates, which often gives rise to a wave of social media posts of victims sharing their stories, and at times even supporting them with evidence [36] . In November 2021 when Chinese tennis player Peng Shuai made allegations of sexual assault against a former senior politician, China's censorship apparatus quickly erased evidence of the social media posts with which she shared her story.[37] As for achieving equality among all ethnicities and religions represented in China, the stories of human rights abuses against Uighur Muslims in Xinjiang [38] obscure this goal and, once again, shed light on the importance of free online communication exchange. It was the latter that focused the attention of the international community on the mistreatment of this minority group, as users started posting pictures of loved ones who had disappeared or were in one of Xinjiang's internment camps.[39]

[29] Ministry of Foreign Affairs of the People's Republic of China, "Whole-Process People's Democracy Is A High Quality Democracy", 11 December 2021, https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zwjg_665342/zwbd_665378/202112/t20211213_10467431.html.

[30] Global Times, "Ten Q&As on Whole-Process People's Democracy - Global Times," December 2021, https://www.globaltimes.cn/page/202112/1241066.shtml.

[31] Amy Qin and Paul Mozur, "China's Silence on Peng Shuai Shows Limits of Beijing's Propaganda," *New York Times*, November 30, 2021, https://www.nytimes.com/2021/11/30/world/asia/china-peng-shuai-propaganda.html.

[32] Emily Feng, "Prominent Critic Of Xi Jinping And Communist Party Sentenced To 18 Years In Prison," *NPR*, 22cSeptember 2020, https://www.npr.org/2020/09/22/915558372/prominent-critic-of-xi-jinping-and-communist-party-sentenced-to-18-years-in-pris.

[33] Chun Han Wong, "China Is Now Sending Twitter Users to Prison for Posts Most Chinese Can't See," *Wall Street Journal*, 29 January 2021, https://www.wsj.com/articles/china-is-now-sending-twitter-users-to-prison-for-posts-most-chinese-cant-see-11611932917.

[34] Amy Qin, "A Prosperous China Says 'Men Preferred,' and Women Lose", *New York Times*, 16 July 2019, https://www.nytimes.com/2019/07/16/world/asia/china-women-discrimination.html.

[35] Center for Strategic and International Studies, "Do Women in China Face Greater Inequality than Women Elsewhere?," *ChinaPower Project* (blog), June 25, 2018, https://chinapower.csis.org/china-gender-inequality/.

[36] Kerry Allen, "Makeup Vlogger Reignites Chinese Domestic Violence Debate", *BBC News*, 28 November 2019, https://www.bbc.com/news/world-asia-china-50578717.

[37] Qin and Mozur, "China's Silence on Peng Shuai Shows Limits of Beijing's Propaganda"

[38] Matthew Hill, David Campanale, and Joel Gunter, "'Their Goal Is to Destroy Everyone': Uighur Camp Detainees Allege Systematic Rape", *BBC News*, 2 February 2021, https://www.bbc.com/news/world-asia-china-55794071.

[39] Amy Mackinnon, "Xinjiang's Voiceless Protests Hit Social Media", *Foreign Policy* (blog), 27 January 2022,

Cyber democracy and the UAE's cybersecurity strategy

The UAE federation of seven emirates along the eastern coast of the Arabian Peninsula is aspiring to become a modern state with enhanced innovation and cybersecurity capabilities.[40] The UAE's constitution states that it 'protects civil liberties, including freedom of speech and press, peaceful assembly and association, and the practice of religious beliefs'.[41] However, there are multiple cases known to the international community in which activists were imprisoned for their anti-government views.[42] In this context lawfulness, a core democratic principle is questioned, as an officially proclaimed constitutional right is violated and the following court processes are unfair and based on forced confessions. [43] Additionally, there is evidence of continued detainment after the completion of sentences, raising further doubts about the state's adherence to the law and its commitment to defending human rights, including those of detainees.[44] The Internet, presenting a wide range of possibilities for communication, is monitored by the government for surveillance purposes and censorship. The state's control over cyberspace includes 'social media, instant messaging services, and blogs with little to no judicial oversight'.[45] Furthermore, there are reports that the UAE employs a trojan called *Remote Control System* (RCS). It was allegedly purchased from an Italian company to target activists, including Ahmed Mansoor, who launched a pro-democracy online petition in 2012. [46] Mansoor was abducted from his home in 2017 and sentenced to 10 years in prison the following year for damaging the 'status and prestige of the UAE and its symbols'.[47]

Another example of the UAE's cybersecurity approach also includes the monitoring of social media posts critical of the UAE's allies. For instance, a UAE national residing in Jordan received a 10-year prison sentence for his Facebook posts criticizing Jordan's government.[48] With this in mind, the expansion of AI tools for facial recognition of alleged suspects [49] raises further concerns about the misuse of cyberspace. While AI has proven to be a powerful asset in the fight against COVID-19

https://foreignpolicy.com/2019/08/21/xinjiangs-voiceless-protests-hit-social-media-china-uighur-uyghur-tiktok/.

[40] The Official Portal of the UAE Government, "Innovation", 23 October 2021, https://u.ae/en/about-the-uae/the-uae-government/government-of-future/innovation-in-the-uae.

[41] The Official Portal of the UAE Government, "Human Rights Are Guaranteed by UAE Constitution", 10 September 2020, https://u.ae/en/about-the-uae/human-rights-in-the-uae/human-rights-are-guaranteed-by-constitution.

[42] Human Rights Watch, "United Arab Emirates: Events of 2020", in *World Report 2021*, 2021, https://www.hrw.org/world-report/2021/country-chapters/united-arab-emirates.

[43] Ibid.

[44] Ibid.

[45] United States Department of State, "2020 Country Reports on Human Rights Practices: United Arab Emirates", 2020, https://www.state.gov/reports/2020-country-reports-on-human-rights-practices/united-arab-emirates/.

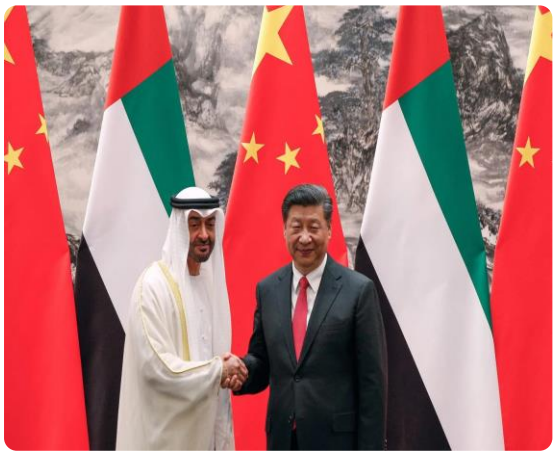
[46] William R Marczak et al., "When Governments Hack Opponents: A Look at Actors and Technology" (23rd USENIX Security Symposium, San Diego, CA, 2014), 511–25.

[47] Amnesty International, "UAE: Ahmed Mansoor, unlawfully detained in solitary confinement for three years, must be released", March 20, 2022, https://www.amnesty.org/en/latest/news/2020/03/uae-ahmed-mansoor-unlawfully-detained-in-solitary-confinement-for-three-years-must-be-released/.

[48] Human Rights Watch, "UAE: Jordanian Convicted For Criticizing Jordan On Facebook", 2021, https://www.hrw.org/news/2021/02/11/uae-jordanian-convicted-criticizing-jordan-facebook.

[49] Ali Aghaddir, "Video: Sharjah Police drones use face-recognition technology to identify wanted criminals", Gulf News, 26 April 2021, https://gulfnews.com/uae/crime/video-sharjah-police-drones-use-face-recognition-technology-to-identify-wanted-criminals-1.78577304.

in the UAE, it has also been deployed for other, less democratic purposes. For instance, the drones adopted by the UAE law enforcement, which are used on a 24-hour basis, may not only serve to expand the government's surveillance capabilities but may also be used for more nefarious purposes, as they are capable of shooting bullets.[50] As the UAE strives to become a leader in AI technology,[51] there are fears such innovation will be further harnessed for censorship and surveillance purposes.



According to the UAE's own data and data from the World Bank, between 76% and 82% of UAE nationals have access to the Internet,[52] which is among the highest rates in the world. The Emirati government has also been working on expanding and enhancing the services it offers through its e-Government portal, making information available to a large percentage of the Emirati population. One study[53] explores the quality of the two-way online communication between government and citizens, supposedly to enable the government to understand the community's needs better. According to the study, while there have been significant efforts by the UAE to reach users and provide greater transparency, information is disseminated without using the full potential of the medium, while also failing to engage stakeholders in the process of need-based decision-making. However, taking into account the number of online users in the UAE and the tools for control over the cyberspace, two aspects are worth considering: 1) what kind of information citizens have access to, given that much of it has been filtered by the government, and 2) to what extent the government monitors online content.

Implications of the China–UAE alliance on cyber democracy

Digital tools give governments new opportunities to repress and disrupt. In non-democracies, the utilization of these tools is known as 'digital authoritarianism'. These tools are used to surveil populations for signs of dissent and to detect political opposition. They are also used to undermine adversaries abroad, extending states' reaches internationally. China is the largest exporter of such tools. At present, China is bidding to become the world's dominant AI superpower. It is one of the most significant tools of China's dominance. Through AI, China is poised to shape the technical standards, values and balance of military and economic power that will

[50] Ibid.

[51] Pat Brans, "Can UAE Become a World Leader in AI?", *ComputerWeekly*, 16 November 2021, https://www.computerweekly.com/news/252509538/Can-UAE-become-a-world-leader-in-AI.

[52] Badreya Al jenaibi, "War and the Worlds and the Promise of Social Media Tools", *Journal of Mass Communication and Journalism* 2, no. 10 (January 1, 2012): 1000130, https://doi.org/10.4172/2165-7912.1000130.

[53] Elsayed B. Darwish, "The Effectiveness of the Use of Social Media in Government Communication in the UAE", vol. 10, no. 1, *Journal of Arab & Muslim Media Research*, 2017, pp. 41–63, https://doi.org/10.1386/jammr.10.1.41_1.

govern the lives of its own citizens and many around the world. Furthermore, China has continued to develop a vast censorship apparatus to stifle free expression and political dissent.

China has been exporting its digital authoritarianism across the world in a number of ways. One of the most high-profile examples is that of the UAE. In the Middle East, where cybersecurity is expanding at an increasing pace, the UAE remains a step ahead. Chinese investment in the UAE comes with a promise to train Emiratis in dealing with public and private cybersecurity threats. Being an asset management and shipping service hub, the UAE has been an obvious cybercrime target, suffering damages to the tune of $1.4bn per year. [54] Chinese investment promises to bolster the local security ecosystem. The Chinese company Huawei is now working with various government agencies to establish the UAE as a 'globally trusted digital oasis' [55] that is safe from potential cyber threats. The Shenzhen-based security firm was also appointed co-chair of the 5G security working group of The Organisation of Islamic Cooperation's computer emergency response team. [56] At the Gulf security expo held in Dubai, Huawei was training the UAE in cybersecurity and is currently attempting to enter public-private partnerships to create a 'robust security system'.[57] Huawei is also one of the main players in the UAE's countrywide installation of 5G networks.

Intensive China-UAE cooperation in the sphere of 5G and AI, part of the Digital Silk Road Initiative of Beijing, [58] could have serious implications for freedom of speech and privacy, not only in the UAE but in neighboring countries as well. China's efforts to spread its 'digital authoritarianism' [59] model - characterized by mass surveillance, the use of artificial intelligence, and networked smart city technology - are likely to continue as more and more states seek out affordable AI and 5G technologies that are useful tools with which to collect data and surveil citizens' daily activities, especially activists who are engaged in human rights campaigns and pro-democracy movements.[60] At the same time, expanding high-quality Internet access may enable a voice for some marginalized communities, but only in the eventuality that they are able to avoid falling under the radar of the state surveillance apparatus. However, considering the advanced technology that China offers, the negative aspect of surveillance and data collection still outweighs the benefits of any

[54] Damian Radcliffe, "Cybercrime: Why Can't the Middle East get to Grips with the Threats?", ZDNet, 13 August 2018, https://www.zdnet.com/article/cybercrime-why-cant-the-middle-east-get-to-grips-with-the-threats/.

[55] Huawei, "Huawei to Help Establish UAE as Cyber Security Hub", 6 June 2021, https://consumer.huawei.com/ph/community/details/Huawei-to-help-establish-UAE-as-cyber-security-hub/topicId_131528/.

[56] Telecom Review, "Huawei Acts as Co-chair at 5G Security Working Group", 1 June 2021, https://www.telecomreview.com/index.php/articles/telecom-vendors/5006-huawei-acts-as-co-chair-at-5g-security-working-group.

[57] Huawei, "Huawei to Help Establish UAE as Cyber Security Hub".

[58] "China's Digital Aid: The Risks and Rewards", *Council on Foreign Relations*, 31 January 2022, https://www.cfr.org/china-digital-silk-road.

[59] Jon Porter, "The NYT Investigates China's Surveillance-State Exports", *The Verge*, 29 April 2019, https://www.theverge.com/2019/4/29/18522248/china-surveillance-state-exporting-ecuador-senain-ecu-911-privacy-facial-recognition-tracking.

[60] Adrian Shahbaz, "The Rise of Digital Authoritarianism" (Freedom House, 2018), https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.

non-political use of new technology if it is ultimately limited and employed for social control purposes. So far, the development of 5G and AI technology has been portrayed mostly as a need-based strategy. While there are undoubtedly advantages for online users, if this technology is manipulated to serve the interests of a small group of people in power, it cannot be labeled as a need-based policy as the latter is a core principle of a modern, democratic cyber society.

Legally, there are similarities in how the UAE and China treat cybercrimes. A report by Freedom House notes that the use of restrictive laws in China, which were implemented under the pretext of preventing cybercrime, in reality, are used to curtail free speech and are mimicked by other countries in Africa and Asia as well.[61] Concerns about such legislation exist, not only for non-democracies, where it is most expected to appear but also in democratic countries, including the US, where Internet freedom has continued to decrease in the five years prior to 2021.[62] Among the issues lowering its score are limited Internet access, alongside access to content protected by the standards of international human rights, as well as violations of users' privacy rights. [63] Instead of promoting accountability through cyberspace, the opposite approach has been observed in China – preventing accountability through the 'managing' of public opinion and the filtering of digital content. Evidence of this is the 'Seminar on Cyberspace Management for Officials of Countries along the Belt and Road Initiative', during which strategies for real-time control of public opinion were discussed, along with the promotion of a 'positive energy public-opinion guidance system'.[64] Participants in these seminars included representatives of various Arab countries; including, notably, the UAE.[65] As the UAE continues to covet closer ties with China, technological collaboration in the realm of cybersecurity is likely to be a key component.

[61] Ibid.

[62] Freedom House, "United States: Freedom on the Net 2021 Country Report", Freedom House, 2021, https://freedomhouse.org/country/united-states/freedom-net/2021.

[63] Ibid.

[64] Shahbaz, "The Rise of Digital Authoritarianism".

[65] Ibid.

II. ELITE HACKING AND CORPORATE ESPIONAGE: COMPARING THE CHINESE AND THE UAE AUTHORITARIAN MODUS OPERANDI OF USING PROXIES IN CYBERSPACE

Metodi Hadji-Janev

The early libertarian optimism about cyberspace and information and communication technologies' decentralizing and democratizing effects are long gone. Liberal virtues (open market, outsourcing, knowledge and technology transfer, open access to information, etc) and modern technologies - once considered to be the drivers of transformative democratic forces - have become an authoritarian 'playtoy'. By abusing modern technologies, autocratic regimes such as China or the United Arab Emirates can control information flows and use intrusive methods and technologies against peer competitors and domestic opposition, while uniquely exploiting the openness of democracies. Using state proxies in cyberspace for political objectives provides authoritarian regimes with an asymmetric advantage at the expense of complex challenges to aspirations and efforts for liberal cyber governance. In sum, authoritarian regimes use proxies for elite hacking and corporate espionage for political purposes. They exploit altering cybersecurity reality to corrupt promising democratic processes to their advantage.

The changing security reality in cyberspace and the opportunities for authoritarian regimes

The ongoing digitalization and the accelerated convergence of cyber and physical space propelled the world into an era where rapid technological development and structural innovation fundamentally altered the way that individuals and governments interact. While these processes have accelerated innovation and brought benefits and commodities, the many lucrative opportunities have uniquely challenged national security. By fusing emerging and disruptive technologies with increasingly sophisticated strategies into a new threat vector, authoritarian regimes have proven keen to, and capable of, fundamentally opposing, altering, or even destroying the post-Westphalian, UN structured rules-based international order and its system of values.[66] As a result, cyberspace has turned into a digital

[66] The most recent transformation of world order is often epicted as a shift from a Westphalian to a post-Westphalian era in which international organizations are becoming increasingly independent sites of authority. More about these approaches to international relations and state power see in Falk Richard, " Revisiting Westphalia, Discovering Post-Westphalia", The Journal of Ethics Vol. 6, No. 4, Springer (2002), pp. 311-352, available at: https://www.jstor.org/stable/25115737

battleground, where nation-states and their proxies, organized criminal groups, terrorists, hacktivists and others seek to gain an advantage over one another.[67]

Interconnectivity and interdependence, along with the spread of advanced technologies and their potential to cause cascade effects, introduced the unprecedented power of asymmetry. [68] State regimes that were lagging behind in military advantage and technological competitiveness learned that the convergence between the cyber and physical space has left many constructual (in terms of technology but also in terms of policies) voids. [69] While the post-Westphalian rule-based international order codified in the UN Charter has generated norms to regulate relationships between states in the physical space, these norms are hardly applicable in cyberspace.[70] When they are, these regulations significantly challenge established concepts (both security and political). Summarising state practice in cyberspace, Betz and Stevens[71] argue that the behavior of both liberal democracies and authoritarian regimes in cyberspace is, in fact, very similar. According to them, 'what is rarely discourse is that recent moves by democratic governments into these regulatory spaces have much in common with the practices of other states whose regimes are often the subject of Western opprobrium and condemnation.'

Nevertheless, while it is true that liberal democracies struggle with the challenges stemming from cyberspace and state control, accountability and checks and balances do not exist in authoritarian regimes' practices. For example, the Investigatory Powers Bill, introduced by the United Kingdom and seen as one of the most far-reaching Internet surveillance laws in a democratic state, was struck down by the European Court of Justice as being in violation of democratic norms.[72] Arguably, in the foreseeable future, we will never see such a decision in China, Russia, Saudi Arabia or the UAE. Moreover, as structural (conventionally understood) power in cyberspace erodes and states lose their monopoly on power; in order to accomplish their political objectives, authoritarian regimes continue to chase opportunities across multiple domains via cyberspace.

---

[67] Alexander Keith, Jaffer Jamil, and Brunet Jennifer, "Clear Thinking About Protecting the Nation in the Cyber Domain," The Cyber Defense Review vol. 2, no. 1 (2017): 29-38

[68] See broader discussion on the subject in Clemente Dave, Cyber Security and Global Interdependence:

What Is Critical?", Chatham House (The Royal Institute of International Affairs), 2013, available at: https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/0213pr_cyber.pdf

[69] Larry M. Wortzel, " China's Military Modernization and Cyber Activities: Testimony of Dr. Larry M. Wortzel before the House Armed Services Committee", Strategic Studies Quarterly Vol. 8, No. 1 (SPRING 2014), pp. 3-22

[70] For a broader discussion on the subject see Delerue François, "Cyber Operations and International Law", Cambridge University Press, 2020, (Particularly Ch.1 Does International Law Matter in Cyberspace?). For early influential writings also see: Schmitt N. Michael, "The Use of Cyber Force and International Law? In *The Oxford Handbook of the Use of Force in International Law* Ed. by Marc Weller, 2016, Oxford University Press; also see Nicholas Tsagourias, (2016) Non-state actors, ungoverned spaces and international responsibility for cyber acts, Journal of Conflict and Security Law, 21 (3). pp. 455-474, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3242718

[71] David J. Betz and Tim Stevens, "Cyberspace and the State: Towards a Strategy for Cyberpower (Adelphi series) (1 ed.). (2012), New York: Routledge

[72] Emma Woollacott, "UK joins Russia and China in legalizing Bulk Surveillance", Forbes, (November 18, 2016), available at:

http://www.forbes.com/sites/emmawoollacott/2016/11/16/uk-joins-russia-and-china-in-legalizing-bulk-surveillance/#37d08afa65f

The low barriers of entry into cyberspace allow authoritarian regimes to have effective capabilities against networks of information and communication technologies.[73] In addition to this, another disturbing trend that offers an opportunity for authoritarian regimes (related to activities via cyberspace but separate from the emergence of cyberspace) is the privatization of national security - a trend that has become increasingly evident in the past 30 years. Namely, this liberal-driven logic has incentivized the majority of Western states and their allies to outsource and become highly dependent on private corporations for logistics, research and development. Instead of national security priorities based on the market-driven efficiency framework, liberal governments' decisions are influenced by commercial concerns and lobbying. Hence, profit instead of citizenship and patriotism drives crucial logistics and service suppliers and providers.[74]

Under these circumstances, authoritarian states have significantly invested in cybercrime and corporate espionage capacity building.[75] Furthermore, building on this accessibility and anonymity, authoritarian regimes have proved capable of utilizing complex and hardly identifiable practices immersed under liberal virtues, such as the open market, outsourcing, knowledge and technology transfer, and open access to information to hide their activities and ambitions.[76]

Thus, while they are able to inflict tremendous social and economic harm, they persistently erode democratic states' capacities to effectively function and respond accordingly.[77] These practices allow them to blend military and civilian operations, exploit critical infrastructures' vulnerabilities (run by private corporates), stay under the radar of national security defenders, and confuse liberal democratic policymakers and responders.[78] Moreover, authoritarian regimes such as those who seek to challenge the liberal world on a global scale: China[79], or those who, at least for now, are just pursuing their own agenda: UAE,[80] have shown a growing interest in using cybercriminals (state coordinated and employed, or freelancers) and proxies for hire to leverage capabilities that previously only governments possessed.[81] Recent

---

[73] Bremmer Ian, "Democracy in Cyberspace: What Information Technology Can and Cannot Do", Foreign Affairs

Vol. 89, No. 6, The World Ahead (November/December 2010), pp. 86-92

[74] Stephen E. Flynn, "America the Vulnerable", HarperCollins, 2004, p.5

[75] Paola Tessari and Karolina Muti, "Strategic or critical infrastructures, a way to interfere in Europe: state of play and

Recommendations", European Parliament, Policy Department for External Relations, July 2021, availabel at: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653637/EXPO_STU(2021)653637_EN.pdf

[76] See more about how anonymity challenges democracy in: Yaman Akdeniz, "Anonymity, Democracy, and Cyberspace", Social Research Vol. 69, No. 1, Privacy in Post-Communist Europe (SPRING 2002), pp. 223-237

[77] Joseph Nye, (November 13, 2018), "Protecting Democracy in an Era of Cyber Information War", Governance In An Emerging New World, Fall Series, Issue 318, available at: https://www.hoover.org/research/protecting-democracy-era-cyber-information-war

[78] Ibid

[79] Adam Segal, "Attribution, Proxies, and US-China Cybersecurity Agreement", Council on Foreign Relations, September 28, 2015, available at: https://www.cfr.org/blog/attribution-proxies-and-us-china-cybersecurity-agreement

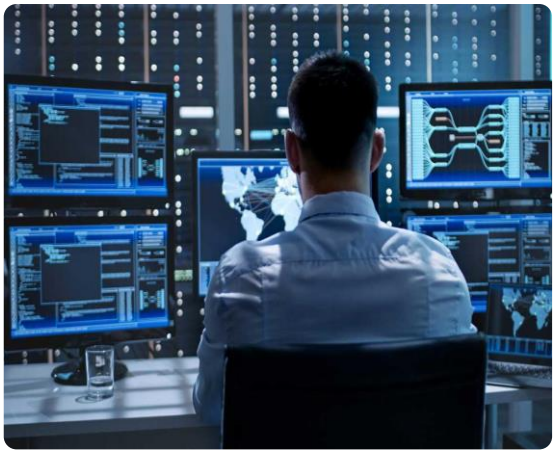
[80] Nima Khorrami, "The Great Power Race in GCC Cyberspace", Carnegie Middle East Center, (December 14, 2020), available at: https://carnegie-mec.org/sada/83446

[81] Madelyn Creedon, "Space and Cyber: Shared Challenges, Shared Opportunities: Edited Remarks to the USSTRATCOM Cyber and Space Symposium: 15

trends, of exploiting legal voids and hiring elite Western-trained hackers (a practice notoriously utilized by the UAE) free on the open market, raise serious concerns and urge closer attention to address the issue of proxies and cyber mercenaries.

Proxies and cyber mercenaries: a toolkit for authoritarian regimes

The possibility of accomplishing political objectives at a low cost (both in financial and political contexts) is a powerful incentive that has driven states to opt for substantive force rather than the national regular one. Traditionally these practices, known as subsidiary or proxy forces, have been understood as engagements wherein a third party is used to achieve an outcome in favour of its sponsor.[82] This strategy is an attractive option for countries seeking to avoid high costs, but also for those who want to compensate for their military and technological disadvantages. In fact, authoritarian state actors have quickly understood that Western liberal national security and corporate espionage practice is often met with an unparalleled response.



Proxies or cyber mercenaries prove that it is easy to manipulate entire nations, even regions. The ability to exploit technical glitches or build on the questionable market-based algorithms designed for profit generate major challenges to democracy.[83] Capitalizing on modern-day residual challenges, cyber mercenaries or proxies prove capable of pushing citizens into polarized echo chambers, while also pulling at the social fabric of a country, fueling hostility between different communities. [84] While disinformation practices have largely been addressed by Western governments, other trends of abusing cyberspace for political gains at the most senior levels of liberal governments have an unmatched understanding of the

November 2011," Strategic Studies Quarterly vol. 6, no. 1 (2012), p. 3-8

[82] For example in In Chinese history, the 36 stratagems include one recommending 'Kill with a borrowed sword. According to an article published by the Shanghai Daily in 2013, 'the true meaning of this stratagem is to attack your enemy by using the forces or strength of a third party, or to entice your ally into attacking your enemy instead of doing it yourself. Please see: "Thirty-Six Stratagems Ancient ruses can still be useful", Shanghai Daily (Shanghai, July 7, 2013), available at: https://archive.shine.cn/sunday/now-and-then/%E4%B8%89%E5%8D%81%E5%85%AD%E8%AE%A1-ThirtySix-Stratagems-Ancient-ruses-can-still-be-useful/shdaily.shtml; See also RK Cragin, 'Semi-Proxy Wars and US Counterterrorism Strategy' (2015) 38 Studies in Conflict & Terrorism 311; Michael A. Newton, "War by Proxy: Legal and Moral Duties of Other Actors Derived From Government" Case Western Reserve Journal of International Law Vol.37 Issue 2, 2006, available at: https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1367&context=jil; or Geraint Hughes "A Proxy War in Arabia: The Dhofar Insurgency and Cross-Border Raids into South Yemen" The Middle East Journal Vol 69, No.1, (2015)

[83] Proxies and cyber mercenaries are either changing colors or are using the preset environment as described in the Zuboff concept of market capitalism to run operations for profit. Namely, in her original thinking and research state of the artwork Zuboff vividly brings to life the consequences as surveillance capitalism advances from Silicon Valley into every economic sector. Vast wealth and power are accumulated in ominous new "behavioral futures markets," where predictions about our behavior are bought and sold, and the production of goods and services is subordinated to a new "means of behavioral modification.". Zuboff Shoshana,, "The Age of Surveillance Capitalism", 2019

[84] Adrian Shahbaz, "The Rise of Digital Authoritarianism", Freedom House, 2018, available at: https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism

current cyber, espionage, and national security risk and regulatory landscape.

Authoritarian regimes have learned that democracies are famously slow at responding to crises. The cornerstone of democracy translated into a system of checks and balances, open deliberation, public participation and dependence on public opinion, can hardly cope the with rapid decision-making necessary to address the challenges that stem from cyberspace. These in-built approaches combined with internal corruption and organized crime schemes have helped some semi-democratic countries fend off authoritarian-style Internet controls over the past years.

As a result, authoritarian regimes have the capacity to silence their citizens in the diaspora through digital threats, coercion by proxy and spyware. In its 'Out of Sight, Not Out of Reach' report, Freedom House revealed that transnational digital authoritarianism is particularly subtle, pernicious, and low-cost since it circumvents issues of national sovereignty and does not require travel or direct government involvement.[85] The problem is even more alarming given that, according to Steven Feldstein, there is no evidence of a grand intentional strategy to 'systematically proliferate digital authoritarian tools'. [86] Instead, as Shoshana Zuboff describes through her con[cept of surveillance capitalism, the use of surveillance and tracking has become a feature of many of the technologies present in the everyday liberal democratic environment.[87]

Moreover, the proliferation of dual-use cyber tools on the open cyber market has pushed authoritarian regimes to pursue lucrative opportunities that are, in turn, reshaping the cyber threat landscape. Offensive and intrusive cyber tools developed purposefully or gained through the open market allow for unprecedented espionage and surveillance capabilities, which are often the precursors to criminal financial gain, destruction and disruptive operations. By utilizing liberal style open market techniques through government-run companies, authoritarian regimes such as China or Russia can flood the market with both surveillance software and related capabilities - hardware needed to run certain software.

Recruiting and building or using 'off-the-shelf' capacities (proxies or cyber mercenaries) of elite hackers by authoritarian states is not a secret. In its 2021 report, the UN Working Group (UNWG) on Mercenaries provides a framework for distinguishing between two types of companies acting as proxies: (1) large technology platforms supporting governments to access information and run surveillance programs, and (2) smaller companies providing tailored services and

[85] Out of Sight, Not Out of Reach report, Freedom House, available at: https://freedomhouse.org/sites/default/files/2021-02/Complete_FH_TransnationalRepressionReport2021_rev020221.pdf

[86] "When it comes to digital authoritarianism, China is a Challenge — But Not The Only Challenge", War on the Rocks, (February 12, 2020), available at: https://warontherocks.com/2020/02/when-it-comes-to-digital-authoritarianism-china-is-a-challenge-but-not-the-only-challenge/

[87] Shoshana Zuboff, "The Age of Surveillance Capitalism"

specific capabilities for conducting malicious operations.[88]

Authoritarian regimes like China, Russia and Iran dedicate significant efforts to establishing state-controlled hacker forces. Another emerging trend producing disruptive challenges in cyberspace stems from the opportunity to buy cyber tools or cyber experts, or partners on a commercial basis. Smaller but richer authoritarian regimes such as the UAE or Saudi Arabia have made outsourcing their preferred method. Saudi Arabia's cyber arsenal is believed to be primarily composed of outsourced espionage tools, which it has combined with disinformation tactics on social media. In addition to purchasing cyber capabilities, Saudi Arabia has also become adept at deploying disinformation campaigns, largely aimed at discrediting its enemies.

A closer look at China's cyber proxy practices

A brief overview of China's deployment of proxies indicates a highly complex and orchestrated methodology that blends and corrupts liberal virtues, and the concept of governing that has dominated international affairs since the end of the Cold War. China represents an excellent case study to trace how a state moves from permitting the malicious behavior of hackers to building orchestrated structures of private actors or, as Tim Maurer describes, 'to tighten the leash and evolve from orchestration to delegation'.[89]

Cyber proxies in China followed the government's allowance of a growing number of hacktivists. Later, this practice evolved into a fully institutionalized militia system. [90] Understanding the contextual geostrategic power that cyberspace and ICT can offer, China's leadership was among the first that augmented the civilian dimension for political potency. Arguably, this is one of the spheres where Chinese corruption of liberal virtues first emerged. While some argue that increased civil-state (military) relations in China's internal affairs represented a historical precedent, in many ways, it also served as a power fusion methodology to centralize power.[91]

[88] The UN General Assembly, "Report of the Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the right of peoples to self-determination", July 15, 2021, available at: https://undocs.org/A/76/151

[89] Tim Maurer, "Cyber Mercenaries, The State, Hackers, and Power", 2017, p.107

[90] See some early reports on the issue by Harris Shane, "Chinese hackers pose a clear and present danger to the US", government and private-sector computer networks and may be responsible for two major US power blackouts", NextGov, available at: https://www.nextgov.com/cio-briefing/2008/05/chinas-cyber-militia/42113/

[91] Michael Kiselycznyk and Phillip C. Saunders, "Civil-Military Relations in China: Assessing the PLA's Role in Elite Politics", National Defense University Press, Washington, D.C, 2010, available at: https://inss.ndu.edu/Portals/68/Documents/stratperspective/china/ChinaPerspectives-2.pdf

The Chinees doctrine of utilizing civilian power dates back to Mao Zedong's People's War. This doctrine, in many ways, builds on the idea that China's military advantage lies in utilizing and mobilizing the vast Chinese population. China's 'patriotic hackers' are perhaps the most well-known face of cyber militias.[92] In practice, these proxy forces are adept at targetting state adversaries, but they are also highly unruly, erratic and heavy-handed. Building on its popular nationalism – often defined by effusive, unsubtle and rash pursuits, China exploited these proxies in the early stages of cyber power projection.[93] The Red Hacker Alliance, which initially received little media attention was, in fact, responsible for many of the headline-grabbing accounts of 'Chinese hacker attacks', in response to the 1998 ethnic riots in Jakarta, Indonesia.[94] As a civilian organization, the Red Hacker Alliance demonstrated how nonstate actors can provide the government with plausible deniability.

Later, China started to exploit this option at a more organized level. The second period in China-proxy relations is, therefore, characterized by orchestrating non-state actors' behavior to enhance its own power projection, in order to short cut its disadvantage against the USA and other Western democracies. To bolster the centralization of power, China developed the so-called 'corporate state model'.[95] This model was supposed to help China's leadership catch up with the global trend of relentlessly pluralizing society. To prevent centrifugal and opposing forces from growing, China utilized this model to co-opt and direct the behavior of these entities in order to prevent the proliferation of autonomous action, perceived as inherently threatening to stability and one-party rule. Appealing to the nationalist motivations of these civil society actors, and seeking to weave them into a more tightly controlled machine, state nationalism, which was designed to empower these movements, only resulted in controlling them.

Externally, this methodology was a force multiplier. Building on the attribution challenge, China started to frequently use state proxies to compensate for its inferiority, particularly in relation to the US. Back in December 2005, as accusations of China's involvement in government-sponsored hacking intensified, China's Foreign Ministry spokesman, Qin Gang, flatly denied charges of government involvement, asking the US to produce any information proving these allegations. According to Scott Henderson, one of the most influential figures in Chinese cyber affairs, Chinese officials pushing the US to reveal evidence was highly effective at deterring further inquiry. Such an approach requires a Chinese Trojan database to reveal specific incidents and explain the

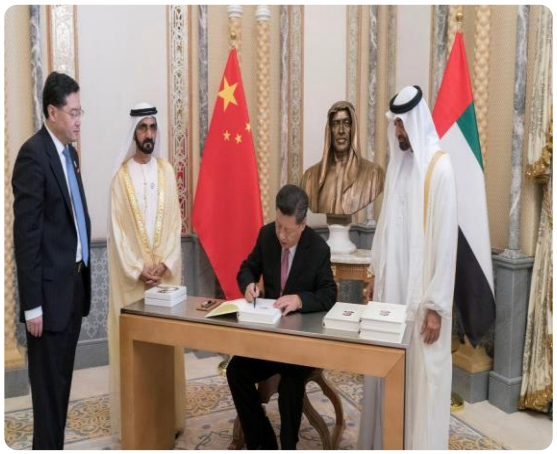
[92] Lorand Laskai, "When China's White-Hat Hackers Go Patriotic", The Council on Foreign Relations, March 13, 2017, available at https://www.cfr.org/blog/when-chinas-white-hat-hackers-go-patriotic

[93] Eric Donelly, "The United States-China EP-3 Incident: Legality and "Realpolitik", Journal of Conflict & Security Law Vol. 9, No. 1 (Spring 2004), pp. 25-42

[94] The Indonesian populace unfairly blamed their ethnic Chinese community for the country's out-of-control inflation. Indonesian citizens turned on the Chinese living among them, committing murders, rapes, and destruction of businesses. News of these atrocities filtered back to individual Chinese hackers, who in retaliation formed the "Chinese Hacker Emergency Conference Center," sending e-mail bombs to Indonesian government websites and mailboxes and conducting Denial-of-Service (DoS) attacks against Indonesian domestic sites.

[95] Philippe C. Schmitter, "Still the Century of Corporatism?"

techniques that led to those conclusions, thereby revealing US operational capabilities in intrusion detection, backtracking and identifying attacking points of origin.[96]



Profiling cyber intrusion by Chinese state-sponsored groups since 2004, Mandiant, a cyber security company from the US (which has since been purchased by FireEye), in 2014 published a report revealing information about the group known as 'Unit 61398'. According to the report, this group was classified as an advanced persistent threat (APT) and was allegedly connected to nearly 150 victims over seven years.[97] The group is believed to be the Second Bureau of the PLA's General Staff Department's Third Department, which is usually recognized by the military label 'Unit 61398'.[98]

This and cases such as Operation Aurora (2009-2010) - a sophisticated and targeted attack on Google infrastructure resulting in the theft of intellectual property from Google, and affecting 15 other companies;[99] Operation Shady Rat (2006-2010) - the biggest transfer of wealth in history at that time);[100] Deep Panda (2011-2015);[101] Operation Poisoned Hurricane (2014),[102] or Emissary Panda (2010-Present)[103] and some others marked the second generation of China-proxy relations evolving from loosely controlled hacker groups to an orchestrated partnership. The recent development of China's cyber power projection through proxies has become more complex and synchronized with China's global reach ambitions. This

---

[96] Scott Henderson, "Beijing's Rising Hacker Stars…How Does Mother China React?", I Sphere, fall, 2008

[97] Dan McWhorter, "Exposing One of China's Cyber Espionage Units", Mandiant Inc. APT1, 2014, available at: https://www.mandiant.com/resources/apt1-exposing-one-of-chinas-cyber-espionage-units

[98] Ibid.

[99] Erica Naone, "Google Reveals Chinese Espionage Efforts." MIT Technology Review. January 13, 2010. available at: https://www.technologyreview.com/2010/01/13/206691/google-reveals-chinese-espionage-efforts/

[100] William Worrall, "The Biggest Hack in History – Operation Shady RAT", Hacked, (March 15, 2021), available at: https://hacked.com/the-biggest-hack-in-history-operation-shady-rat/

[101] A sophisticated cyber espionage operation that attacked health care companies and stoll financial and medical records of approximately eleven million individuals. See for example A Little Sunshine. "China To Blame in Anthem Hack?" Krebs on Security RSS. February 6, 2015, Available at: http://krebsonsecurity.com/2015/02/china-to-blame-in-anthem-hack

[102] An attack in which hackers used malware that was connected to websites like adobe.com and outlook.com, but individuals were re-routed to pages that hackers had set up to look legitimate. See for example, Kovacs Eduard, "APT Group Hijacks Popular Domains to Mask C&C Communications: FireEye.", Security Week, (August 6, 2014) available at: http://www.securityweek.com/apt-group-hijacks-popular-domains-mask-cc-communications-fireeye

[103] Also know as "APT27", "TG-3390", "Bronze Union", "Lucky Mouse" is a Chinese threat group that has extensively used strategic Web compromises to target victims. The group has been active since at least 2010 and has targeted organizations in the aerospace, government, defense, technology, energy, and manufacturing sectors. As well as targeted attacks against other miscellaneous organizations around the world. Allegedly in 2015 and 2016, they continued to use known backdoors associated with them previously, including OwaShell & Wonknu. In 2017 & 2018 they have been notable for their targeting of Turkish organizations, and their use of older backdoors such as ZxShell and Gh0st see more in: UNIT 42, "Emisary Panda", available at https://pan-unit42.github.io/playbook_viewer/?pb=emissary-panda

approach wholeheartedly leverages the civilian sphere and, more importantly, is designed to support China's rise. What we face now is what Tim Maurer classifies as a state of 'delegation' in which the government exerts the greatest degree of control over its proxies.[104]

While practicing elite hacking techniques is still in the game, proxies now play an important role in China's ambition to impose an alternative to liberal democratic governance. Put another way, through state-controlled corporates, China is putting its exporting ideology into practice. [105] For example, Chinese companies are playing a prominent role in the country's push for telecommunications dominance as part of the plan to achieve global influence in cyberspace.[106] This is particularly related to the race in 5G technology. Huawei, for example, is building Latin America's largest public Wi-Fi network in Mexico, Bangladesh's 5G mobile network, and Cambodia's 4.5G service, and is advising the Kenyan government on its 'master plan' for information and communication technologies.[107] As Chinese firms build the 'Digital Silk Road', linking host nations through fiber-optic cables, experts have warned that the equipment may facilitate surveillance by Chinese intelligence services.[108]

Some of the Chinese companies involved are focused explicitly on exporting surveillance technology. In 18 of the 65 countries assessed by Freedom House — including Zimbabwe, Singapore and several Eurasian countries — enterprises such as SZ DJI Technology Co. Ltd., Cloudwalk, Yitu, and the partly state-owned Hikvision are combining advances in artificial intelligence and facial recognition to create 'Smart Cities' and sophisticated surveillance systems. This, without consent, allows authoritarian-leaning governments to identify and track citizens' everyday movements. Last December, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) identified eight Chinese technology firms pursuant to Executive Order (E.O.) 13959, as amended by E.O. 14032., actively supporting the biometric surveillance and tracking of ethnic and religious minorities in China.[109]

---

[104] Tim Maurer, "Cyber Mercenaries: The State, Hackers, and Power, Cambridge, U.K.: Cambridge University Press, 2018

[105] Speaking at the Chinese Communist Party Congress in October 2017, President Xi Jinping publicly outlined his plan to transform China into a "cyber superpower." He offered up the country's model of governance—including its management of the Internet—as "a new option for other countries and nations that want to speed up their development while preserving their independence." See more at China's Approach to Global Governance, see for example in Russ Jevin, "Xi Jinping, China and The Global Order: The Significance Of China's 2018 Central Foreign Policy Work Conference", An Address To The Lee Kuan Yew School Of Public Policy National University Of Singapore, available at: https://asiasociety.org/sites/default/files/2019-01/Xi%20Jinping_China%20and%20the%20Global%20Order.pdf

[106] Chinese companies installed Internet and mobile network equipment in at least 38 countries. Some of these firms are private enterprises and may have their own reasons for making such investments, but all are also beholden to the government and its strategic goals. State-owned China Telecom, China Unicom, and China Mobile are laying down the digital Silk Road, with fiber-optic links to Myanmar, Kyrgyzstan, and Nepal, among other countries. A company called H3C has already won contracts to build the telecommunications network for airports in Nigeria and the port of Gwadar in Pakistan. See more in Adrian Shahbaz, The Rise of Digital Authoritarianism, Freedom House, 2018, available at https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism

[107] Michael Abramowitz and Michael Chertoff, The global threat of China's digital authoritarianism, November 1, 2018, The Seattle Times, available at https://www.seattletimes.com/opinion/the-global-threat-of-chinas-digital-authoritarianism/

[108] Ibid

[109] US Department Of The Treasury, Treasury Identifies Eight Chinese Tech Firms as Part of The Chinese Military-Industrial Complex, (December 16, 2021), acailable at: https://home.treasury.gov/news/press-releases/jy0538

Addressing the decision, the US Under Secretary of the Treasury for Terrorism and Financial Intelligence, Brian E. Nelson, underlined that this action highlights how private firms in China's defence and surveillance technology sectors are actively cooperating with the government's efforts to repress members of ethnic and religious minority groups. [110] Another important concern stems from the fact that as more of the world's critical telecommunications infrastructure is built by China, global data may become more accessible to Chinese intelligence agencies through both legal and extralegal methods.

The UAE cyber-proxy alliance

The case with the UAE's use of cyber mercenaries underscores why states use hackers as proxies to project power through cyberspace. It depicts how small states (geographically speaking) can compete for influence and power projection, abusing modern technologies while also challenging liberal-dominated free-market opportunities. The UAE's aspiration to become a powerful regional tech hub has enabled it to harness greater influence and domination in the region. The UAE has branched into developing its own home-grown surveillance technology by recruiting private digital mercenaries. Initially, the problem with the UAE's ambition was that the monarchy did not have the know-how, nor the technology. However, they did have cash and friends.

In 2016, 'Project Raven' was established. The team was managed by a cybersecurity contractor and made up of former NSA agents. But in 2016, the Emiratis moved Project Raven to a cybersecurity firm named DarkMatter. Before long, Americans involved claimed that they were tasked with targeting fellow American citizens for surveillance. Project Raven used a hacking tool called 'Karma', which can access a phone without the target clicking on a link. It relies on an undisclosed vulnerability in Apple's iMessage system. The story of Project Raven reveals how former US government hackers have employed state-of-the-art cyber-espionage tools on behalf of a foreign intelligence service that spied on human rights activists, journalists and political rivals.

American spies at DarkMatter were crucial in building the UAE's intelligence apparatus capacities for identifying groups and high-profile individuals to be targeted, including Yemeni activists and the Emir of Qatar.[111] In order to camouflage the Project's activities, DarkMatter's chief financial officer Samer Khalife reportedly moved some Americans

[110] Ibid

[111] Jenna McLaughlin, "Deep Pockets, Deep Cover The UAE Is paying Ex-CIA officers to build a spy empire in the Gulf", Foreign Policy , (December 21, 2017), available at: https://foreignpolicy.com/2017/12/21/deep-pockets-deep-cover-the-uae-is-paying-ex-cia-officers-to-build-a-spy-empire-in-the-gulf/

from DarkMatter to a new company, Connection Systems.[112] The purpose of the new company, according to an Intercept investigative report, was to create the appearance that DarkMatter no longer conducted surveillance and cyber operations on behalf of the Emirati government.[113] Connection Systems today employs multiple former DarkMatter staffers, according to LinkedIn.

While DarkMatter officials initially denied these allegations,[114] a US Department of Justice report confirmed them. [115] Furthermore, according to court documents, the defendants worked as senior managers at a UAE-based company that supported and carried out computer network exploitation (CNE) operations - (i.e., 'hacking') for the benefit of the UAE government between 2016 and 2019. Despite the fact that their work for the UAE company, under the International Traffic in Arms Regulations (ITAR) constituted a 'defense service' requiring a license from the State Department's Directorate of Defense Trade Controls (DDTC), the defendants proceeded to provide such services without a license.[116]

Moreover, Acting Assistant Attorney General for the Justice Department's National Security Division, Mark J. Lesko, asserted that, legally, these activities constitute two distinct types of criminal activity. First, they provide unlicensed export-controlled defense services in support of computer network exploitation. Second, the commercial company creating, supporting and operating systems is specifically designed to allow others to access data without authorization from computers worldwide, including in the United States. He also underlined that 'Hackers-for-hire and those who otherwise support such activities in violation of US law should fully expect to be prosecuted for their criminal conduct.'[117]

A brief analysis of contemporary state-proxy practices in cyberspace

The evolving practice of hiring private entities to accomplish strategic objectives via cyberspace (for various reasons from avoiding the applicability of international law, to maintaining plausible deniability by avoiding accountability) is a troublesome concern that fuels uncertainty amidst ongoing geostrategic competition. What also raises serious concerns for Western democratic societies is that regimes considered to be partners (UAE and Saudi Arabia) have utilized similar aggressive behavior in cyberspace. At the same time, the ability of national security and defense agencies - organizations that run critical infrastructures and individuals to patch their systems - cannot keep pace with the new applications of technology, and the speed with which threat actors can find and exploit

[112] Sam Biddle and Matthew Cole, "Team of American Hackers and Emirati Spies Discussed Attacking", The Intercept, (June 12, 2019), available at: https://theintercept.com/2019/06/12/darkmatter-uae-hack-intercept/

[113] Ibid

[114] McLaughlin Jenna, (December 21, 2017),

[115] The US Department of Justice, "Three Former US Intelligence Community and Military Personnel Agree to Pay More Than $1.68 Million to Resolve Criminal Charges Arising from Their Provision of Hacking-Related Services to a Foreign Government", Office of Public Affairs, (September 14, 2021), available at: https://www.justice.gov/opa/pr/three-former-us-intelligence-community-and-military-personnel-agree-pay-more-168-million

[116] Ibid

[117] Ibid

vulnerabilities. Moreover, as geostrategic competition intensifies, the software architectural design process will continue to be fundamentally flawed and, therefore, more difficult to defend.

The diffused cyber reality immersed in the liberal free-market logic of supply and demand is flooded with the mass proliferation of cyber intrusive tools and fast-evolving technology. Such an environment will likely make it increasingly difficult to distinguish threat actors from each other, and from legitimate network activity. Actors' motivations are blurred, and their tactics, techniques and procedures are not always indicative of their targets.118 It is also possible that cyber experts, including former government or military personnel, may not understand the true nature of the work, or they may choose to turn a blind eye until they have become embroiled in an ethically questionable cyber campaign.119

An investigative report by the news outlet Reuters cites Jonathan Cole, an ex-Raven employee, as the leader of similar operations against non-US targets. Allegedly, Cole 'had no involvement in or first-hand knowledge of efforts to hack Americans or American computer systems, but recalled being warned about these efforts by a concerned American co-worker at the time'. 120 He also recalled that 'Project Raven's leadership falsely claimed that the US government was informed of any incidental surveillance of Americans and that such data was routinely purged from DarkMatter computers.' 121 Moreover, contractors were purposefully led to believe that targeting Americans was done with US authorities' knowledge on the basis of a tit-for-tat exchange of intelligence.122

Under such circumstances, as Shoshana Zuboff asserts, 'the threat has shifted from a totalitarian Big Brother state to a ubiquitous digital architecture: a "Big Other" operating in the interests of surveillance capital. Here is the crucible of an unprecedented form of power marked by extreme concentrations of knowledge and free from democratic oversight.'123 What is even more troublesome is that when these ubiquities challenge lawless virtual environments, with quasi-liberal virtues (such as obscure and manipulative outsourcing, shady private corporates, the unlicenced proliferation of tools, etc.), they become powerful pressure tools against peer liberal democratic competitors below the threshold of war.

This brief analysis of the authoritarian practice of using proxies shows that these actors are state-sponsored but are not officially deemed to be working under state formations. While officially working independently of the state, this lucrative

[118] For example, as the University of Pittsburgh Institute for Cyber Law, Policy, and Security study indicates as a defense contractor one may assume that the target of a cyberattack would be access to the US Department of Defense's secure systems; however, nefarious actors may be just as interested in acquiring employees' personally identifiable information (PII) for fraudulent activities. Analytic Exchange Program, "Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar", University of Pittsburgh Institute for Cyber Law, Policy, and Security, supported by the Department of Homeland Security.

[119] Ibid

[120] Sam Biddle and Matthew Cole, (June 12, 2019), "

[121] Ibid

[122] Ibid

[123] Zuboff Shoshana, "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power", New York: PublicAffairs, 2019, available at: https://www.hbs.edu/faculty/Pages/item.aspx?num=56791

partnership provides these cyber individuals, groups, or formations with the advantage of extensive resources, including time and money to achieve persistence, allowing the capability of achieving global reach using advanced tradecraft.

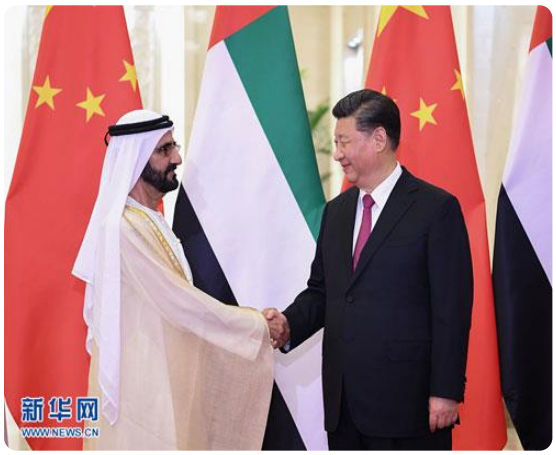
China (but also Russia and Iran) align products, processes and people to these groups and have robust contingency risk management programs to mitigate the effects of exposure. Their 24/7 mission is to collect information, act and attack through multiple domains. Operations are designed, coordinated and arranged with the intent of data collection, surveillance and espionage. A plethora of cyberattack techniques (ranging from malware attacks, phishing, and stalking, to a combination of social profiling and coordinated persistent cyber-attacks) are at their disposal for mission accomplishment. These proxy actors design their own weapons or use off-the-shelf tools (cyber weapons) to target individuals, groups and industries from competitor nation-states. Their targets are usually diplomats, human rights activists and government officials. Operations consist of stealing login credentials, keystrokes, phishing and spear-phishing attacks, SQL Injection Attack, Credential Reuse, Session Hijacking and Man-in-the-Middle Attacks, and Denial-of-Service (DoS).

In practice, these state-sponsored and, sometimes, state-developed proxies have also been deployed in coordination with military efforts and have proved to be a significant force multiplier. While the mission may differentiate initially, capabilities, tools and effects are almost always the same. When combined with remote access and definitive and timely attribution challenges, a fast emerging actor demonstrates a significant threat. These actors could turn geopolitical instability into a conflict in very little time. Unlike traditional military changes in the balance of power, such acquisitions of new weapons and the growing alliance between authoritarian regimes and proxies in cyberspace generate a disturbing burden for liberal democracies to anticipate potential escalation.

The UAE is an interesting example illustrating unprecedented, contextual opportunities. Building and later manipulating Western-based concepts of highly trained individuals employed by liberal democracies in the so-called global war on terror, the UAE has exploited proxies for its own political objectives. Thus, the UAE has borrowed the liberal democratic designed toolkit and has used it in for a completely different purpose, to protect the regime from internal and foreign political opposition or perceived enemies of the state.

The practice of using state proxies in cyberspace provides a lucrative opportunity for authoritarian regimes. In practice, authoritarian regimes use proxies via cyberspace for domestic control and power projection and influence in an ongoing geostrategic competition. China, Russia and Iran dedicate significant efforts to establishing state-controlled proxy hacker forces. Smaller but rich authoritarian regimes such as the UAE and Saudi Arabia have utilized outsourcing, i.e., hackers for higher techniques, thus using off-the-shelf

highly trained nonstate actors and tools under the liberal democratic watch.



The Chinese use of state proxies has evolved through several phases. From loose control and support for 'patriotic hacker' groups and individuals to a fully formed cyber militia, and finally, through to an orchestrated partnership with cyber hacker groups, China today delegates power projection and influence types of missions for state proxies. The UAE case, on the other hand, is an interesting example that illuminates unprecedented contextual opportunities. Building and later manipulating the Western-based concepts of highly trained individuals employed by liberal democracies in the global war on terror, the UAE has exploited proxies for its own political objectives.

While elite hacking practice is about to grow, providing services to clients commonly known to infringe international principles and standards that establish baselines for liberal democratic governance is a serious concern that requires greater attention. Companies and individuals will continue to ignore official warnings and will not hesitate to leverage their years of experience to support and enhance a foreign government's offensive cyber operations. Under these circumstances, liberal democracies need to consider how to adapt their association with proxy groups, or how to protect their capacities which can be used in ways that undermine democracy before it is too late.

III. STATE SURVEILLANCE UNDER HUMAN RIGHTS LAW IN THE CHINA-UAE CYBER SECURITY ALLIANCE

Alexandros Sarris

If activists are to win the fight to keep the Internet free and open, it is becoming increasingly clear that they must familiarize themselves intimately with the areas of cyber security and cyber surveillance. International, state-sponsored cyber espionage has given birth to the twin narratives of cyber war and a cyber arms race; narratives that are being used in some parts of the world to encourage citizens to trade in civil liberties for a greater sense of security. In the US, for instance, incidents of cyber espionage by Chinese hackers form part of a key argument used to support the controversial Cyber Intelligence Sharing and Protection Act (CISPA) which would enable the authorities to access vast amounts of user data without a warrant. Elsewhere, internal threats to national security posed by the use of new technologies have long been used to justify extensive surveillance measures. For example, in India, it is not possible to access mobile phones or Internet connections, including in cyber cafes, without official identification, and both ISPs and cyber cafes are required to maintain detailed logs of users' browsing history. The narratives of doom that invariably accompany such measures draw further strength from the very real growth of cybercrime – there are now said to be more than 150,000 viruses and other types of malicious codes in circulation, with a million people becoming victims of cybercrime every day.[124] So while cyber security is not a new concern, in the last few years it has come to increasingly dominate and drive Internet policy and governance agenda, as well as international policy discourse more broadly.

Genuine threats do indeed exist. Illegal access to computers and data, as well as data interference, have become a more common and complex problem that affects large numbers of people. Issues like fraud are taking new forms on the Internet. And, as more of our critical infrastructure becomes reliant on the Internet, security infringements can have significant repercussions, including for human rights when, for instance, an attack prevents people from accessing public services or exercising their right to free expression. When governments identify security threats

[124] European Commisiom, "Cybercrime", available at: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime/index_en.htm

these should, therefore, not be made light of as a priori. It is an integral duty of any state to ensure the security of the people within its boundaries, and this duty does extend to the cyber domain.

However, cyber security strategies must be designed and implemented in a way that is consistent with international human rights law – too often this is not the case, as seen in the surveillance regimes discussed above. In other cases, states have been found to be behind threats such as cyber attacks aimed at human rights defenders or political opposition. It is therefore important that the broader human rights community starts engaging with these discourses more closely, and to unpack the proclaimed threats as well as their supposed solutions, and to ensure that human rights standards are upheld in the cyber security arena too. In what follows, we hope to contribute to such efforts.

Concerns about current cyber security debates and practices

At present, the term 'cyber security' lacks definition as it is used to cover a vast range of concerns. In different contexts and by different actors, the term is used to refer to the security of national infrastructure; security of Internet infrastructure; security of applications and services; security of users (ranging from businesses to individual users); stability of the state and of political structures. This inexact terminology points to one of the primary concerns about this growing discourse: the terminology covers an agenda that is inexact, mixes legitimate and illegitimate concerns, and conflates different types and levels of risk. This prevents genuine objective scrutiny and inevitably leads to responses that are wide-ranging and which can easily be misused or abused.

Obscuring the role of the state in creating insecurity

Among the important issues that are obfuscated by the current lack of precision in cyber security debates is the fact that rivalries between states are among the chief security threats, with the narratives of cyber war and a cyber arms race rapidly gaining ground at the inter-state level. In particular, a number of countries are reportedly investing heavily in developing offensive capabilities. In recent weeks there have been reports that the Pentagon is fast-tracking cyber weapon development and acquisition through a process separate from that used for conventional weapons. [125] China, too, is considered a major investor in cyber warfare capacity. And in the UK, official statistics show that 59% of the planned spend of the country's Cyber Security Strategy 'is meant to go to the intelligence agencies'. According to a senior officer from Cheltenham, 'GCHQ's

[125] Candice Howarth, "Pentagon's Move to Fast-Track Cyber Weapons Will Upset China and Russia", *MIC*, 4 November 2012, http://www.policymic.com/articles/6730/pentagon-s-move-to-fasttrack-cyber-weapons-will-upset-china-and-russia

offensive capability gives the UK an edge... a large proportion of that money has [therefore] gone into those capabilities.'[126]

Examples of state-sponsored attacks do exist, which states can point to in their arguments about the need for such investment: Russia allegedly launched distributed denial of service (DDoS) attacks that paralyzed Estonia's banking system and civil services during a 2007 diplomatic dispute and, most famously, the United States and Israel allegedly used a computer worm, Stuxnet, to sabotage uranium enrichment facilities in Iran. In both the examples mentioned above, the damage was temporary and the threat could quickly be neutralized, in part because of the amazing resilience of the Internet's architecture. Interestingly, however, the techniques used in such instances are remarkably similar to those deployed by cyber criminals, indicating how governments are exploiting, for their own ends, the very same security breaches that they claim to fight.[127] The language of cyber war and a cyber-arms race has made expanding budgets for the military and intelligence possible at times of general austerity for many countries; contrary to public perception, this is not always for reasons of defence.

Discourses of cyber war and a cyber-arms race have also built a market with lucrative opportunities for the many private businesses that seek to provide the technologies to deal with such purported threats. Indeed, narratives of cyber security prop up not only government power but big business as well, and the influence of the security industry on these debates should not be underestimated. The cyber security sector is estimated to be worth tens of billions of US dollars every year,[128] and they are investing huge amounts of funds in lobbying politicians. A report by the Center for Responsive Politics found that, in the US, the number of lobbying reports which mentioned the term 'cyber security' more than doubled from 2011 to 2012.[129] Industry actors are also behind much of the information driving the agenda; this is extremely problematic given their vested interests. And the relationship between these businesses and governments is often secretive. The sale to authoritarian regimes of technologies that allow for extensive surveillance of citizens by companies based in the democratic world has long been criticized. More recently, a study found that 25 countries were using the surveillance software FinSpy against their citizens, including democratic states. Neither the company, Gamma International, nor the governments involved, disclosed the relationship.[130]

Despite the prevalence of the language of cyber war it is important to remember, however, that the cyber domain is very different from the offline domains (earth, air, sea, space) that the terminology of war comes from, and loaded terms such as 'war' and an 'arms race' are frequently

---

[126] Mark Urban, "Is UK Doing Enough to Protect Itself from Cyber Attack?" *BBC News*, 30 April 2013, http://www.bbc.co.uk/news/uk-22338204

[127] Ronald Deibert, "The Growing Dark Side of Cyber Space (... And What To Do about It), vol. 1, no. 2, *Penn State Journal of Law and Internatinal Affairs,* 2012, pp. 8–12, http://elibrary.law.psu.edu/jlia/vol1/iss2/3

[128] Ibid

[129] Julianne Pepitone, "Cybersecurity lobbying doubled in 2012", *CNN*, 8 April 2013, available at: http://money.cnn.com/2013/04/08/technology/security/cybersecurity-lobbying/index.html

[130] Nicole Perlroth, "Researchers Find 25 Countries Using Surveillance Software", *New York Times*, 13 March 2013, Available at: http://bits.blogs.nytimes.com/2013/03/13/researchers-find-25-countries-using-surveillancesoftware/

inappropriate to describe what is going on. It is far more difficult to localize damage or attribute responsibility online than it is offline. Furthermore, what is often reported in the media as examples of 'cyber wars' do not entail violence and should more appropriately be referred to as instances of 'cyber espionage'. Acts of espionage are usually governed by different legislation than acts of warfare are.

In fact, the only cyber-attack so far that has caused (or is believed to have caused) physical damage offline, and that, therefore, is almost unanimously agreed to be an act of warfare, is Stuxnet, pointing to the duplicitous role that the USA is playing in the cyber security arena. Where governments actively foment reasons for their citizens to fear for their safety unless they accept extensive surveillance measures and offensive capabilities on the part of the state, this is irresponsible governance.

Confusing the debate by conflating different challenges.

More broadly speaking, there are two different types of threat that are conflated all too often in the cyber security debate:

1) Threats where technology is integral to the risk - this category refers to attacks, damage or access without authorisation to data, programs, computers or networks. It includes DDoS attacks, acts of cyber espionage and attacks that aim to sabotage critical infrastructure.

2) Threats conducted over the Internet where it is not fundamental to that risk – this category includes the distribution of spam, the publication of child pornography or the use of the Internet to plan a terrorist attack. In these cases, the issue is not illegitimate access or damage, but consent to the communication (for spam) and the nature of the content of the communication (for child pornography and crimes planned over the Internet). While technology may change the nature or reach of these crimes, it is not integral to their definition as such. By collapsing the two categories for example, by clubbing attacks on critical infrastructure together with spam, which could be regarded more appropriately as an annoyance rather than a threat – the very different nature of the challenges that they entail is obscured. This makes it easy to uncritically supplant the narratives of impending crises that so often link the former to the latter.

Another reason for not conflating cybercrimes in the narrow sense with crimes that merely use the Internet is that it conceals the fact that there are much more clearly defined international standards regarding appropriate responses to the latter than to the former. There remains a paucity of legal analysis using human rights standards of initiatives taken to protect computer systems and networks, including where these form part of the national infrastructure. This is in part because such an analysis would require greater technical knowledge; because the information about these initiatives is often not public; because the impact on human rights standards is therefore often less apparent; and because, until recently, such initiatives were more likely to be private efforts and, thus were less likely to have far-reaching consequences while also being less visible. With countries across the world now adopting cyber security strategies, it is increasingly important that these are analyzed using a human rights legal framework.

In the case of content-related crimes, however, much work has in fact been done

over the past few years – and especially since the publication of the report on the Internet and freedom of expression by UN Special Rapporteur on Freedom of Opinion and Expression Frank La Rue in June 2011 – , to shed light on and develop appropriate responses to content that may seem to fall within the reasonable restrictions on freedom of expression accepted under international law.

However, governments frequently ignore such guidelines. As the Special Rapporteur pointed out in his report, all too often, content restrictions, while potentially legitimate in certain circumstances, are implemented 'without any legal basis, or on the basis of broad and ambiguous laws, without justifying the purpose of such actions; and/or in a manner that is clearly unnecessary and/or disproportionate to achieving the intended aim'.[131] This may well be, at least in part, because the sense of crisis and complexity that surrounds the fields of cyber attacks and cyber warfare is being transferred onto the field of cyber security as a whole.

Big brother in China and the UAE: Surveillance tech's threat to US national security

The development of surveillance technologies has indisputably lent a hand to strengthening the iron grip of authoritarian regimes. Blurring the distinction between the public and private sectors, several governments have used this technology to maintain their political hegemony and inflict human rights abuses. Prominent among these countries is China. In response, the United States placed restrictions on Chinese companies abetting this behavior.[132] With a similar story unfolding in Dubai, where the upsurge of technology has also played into autocratic behavior, the current US administration should curtail certain commercial connections between companies in the United Arab Emirates (UAE) and the United States. Until conditions on the use of these technologies have been agreed upon, the sanctioning of these companies is necessary to both preserve US national security and to uphold democratic principles.

The Chinese government has amassed an arsenal of mass surveillance technology: over 200 million surveillance cameras dot the streets, many of which are equipped with facial recognition capabilities and infrared technology.[133] 'Wifi sniffers' track IP addresses of nearly all networked

[131] Frank Le Rue, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression", Frank La Rue (A/HRC/17/27). New York, United Nations General Assembly, 16 May 2011, para 26. http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

[132] White House, "Executive Order on Securing the Information and Communications Technology and Services Supply Chain", 15 May 2019, https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/

[133] Paul Mozur, "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras", *New York Times*, 8 July 2018, https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html

tools. [134] The thousands of security checkpoints spread out across the country compile information on individuals, ranging from license plate numbers to blood types to family planning. [135] In late 2016, the government released a mobile app as part of the Integrated Joint Operations Program (IJOP). [136] Currently being piloted in the province of Xinjiang, the app streamlines all data received into a single analysis system, enabling the government to easily access a compendium of information on any given individual. The system also documents activity deemed 'suspicious', like possession of an inordinate number of books or an unusually large purchase of fertilizer.[137] In tandem with the social credit system also tested in Xinjiang, by which citizens are assigned a score that determines their social opportunities based on their socioeconomic reputation, the Chinese government has established its presence in nearly every facet of public and private life.

Such an extensive program of surveillance is purportedly targeted towards crime prevention and reduction. In a white paper published in early 2019,[138] officials claimed to have 'destroyed 1,588 violent and terrorist gangs, arrested 12,995 terrorists, seized 2,052 explosive devices, punished 30,645 people for 4,858 illegal religious activities, and confiscated 345,229 copies of illegal religious materials'. The magnitude of the statistics, however, belies the true objectives of the surveillance system: the Big Brother-style of governance aims not only to deter crimes, like petty robberies and traffic infractions but also to stifle what Beijing claims are crimes against the government. The use of surveillance software thus serves an ulterior purpose of clamping down on instances of divergence from the ruling party. 'Terrorists' usually consist of the minority Muslim Uighur people who, on the basis of their religion, are perceived as a menace.[139] 'Gangs' are often simply groups of political dissidents and social activists. By labeling those seen as threats in such pejorative terms, the government justifies its oppressive methods such as its 'reeducation camps' - the conditions of which are not unlike those of concentration

camps - and its systematic use of torture. [140]

[134] Human Rights Watch, "China: Big Data Fuels Crackdown in Minority Region", 26 Feburary 2018, https://www.hrw.org/news/2018/02/26/china-big-data-fuels-crackdown-minority-region

[135] Ibid

[136] Human Rights Watch, "China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App", 1 May 2019, https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass

[137] Nathan Vanderklippe, "China Using Big Data to Detain People Before Crime is Committed: Report", *The Globe and Mail*, 27 February 2018, https://www.theglobeandmail.com/news/world/china-using-big-data-to-detain-people-in-re-education-before-crime-committed-report/article38126551/

[138] Ben Blanchard, "China says 13,000 'terrorists' arrested in Xinjiang since 2014", *Reuters*, 18 March 2019, https://www.reuters.com/article/us-china-xinjiang/china-says-13000-terrorists-arrested-in-xinjiang-since-2014-idUSKCN1QZ08T

[139] Chung, Chien-peng, "China's 'War on Terror': September 11 and Uighur Separatism." *Foreign Affairs*, vol. 81, no. 4, Council on Foreign Relations, 2002, pp. 8–12, https://doi.org/10.2307/20033235.

[140] Chris Buckley and Amy Qin, "Muslim Detention Camps Are Like 'Boarding Schools,' Chinese Official Says", *New*

While the precise motives of the White House remain hazy, several supporters of these restrictions have cited national security concerns and the potential erosion of democratic values. Several high-ranking officials, including chairman of the Senate Intelligence Committee Richard Burr (R-NC) and FBI Director Christopher Wray, have expressed unease regarding the technologies' capabilities to infiltrate the American telecommunication and public infrastructure sectors.[141] The capacity to do so would potentially enable unauthorized access of classified information and expose US vulnerabilities to foreign espionage. This apprehension is not unfounded: an investigation by the French newspaper Le Monde found that the computer systems in the Chinese-built headquarters of the African Union had been sending classified information back to Beijing every day for five years.[142] While there has yet to be such comparable, large-scale Chinese involvement in public infrastructure in the United States, the precedent points to prospective dangers should US companies engage in the unrestrained sale and purchase of Chinese parts.

Further, the application of these tools to stymie any sort of political challenge resulting in flagrant infringements on human rights threatens the principles underpinning democracy. A bipartisan group of senators led by Marco Rubio (R-FL) sent a letter to the Treasury and State Departments calling for restrictions on Dahua and Hikvision contracts on the grounds of the companies' complicity in human rights violations in Xinjiang.[143] To compound this, as Chinese capacities grow, many of these companies, like Hikvision and Huawei, are exporting their products to other countries that are also seeking to centralize power in the hands of their respective autocratic leaders. A New York Times report indicated that at least 18 countries are using Chinese-made surveillance systems.[144] For many, these systems have been provided by the Chinese government as part of its Belt and Road Initiative, headquartering an unprecedented attempt at global surveillance in Beijing.[145] This international system of policing in favour of the Chinese jeopardizes not only the basic rights of those under such regimes but also the international order and norms of sovereignty.

One such country to mirror China is the UAE. In 2016, as part of its Vision 2021 Strategy, Dubai announced plans for Oyoon ('eyes' in Arabic) in cooperation with several high-level governmental ministries.[146] An

York Times, 12 March 2019, https://www.nytimes.com/2019/03/12/world/asia/china-xinjiang.html

[141] Richard Burr, "Burr Statement on Huawei Indictments", *Press Release*, 28 January 2019, https://www.burr.senate.gov/2019/1/burr-statement-on-huawei-indictments

[142] Ghalia Kadiri and Joan Tilouine, "A Addis-Abeba, le siège de l'Union africaine espionné par Pékin", *Le Monde*, 26 January 2018, https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html

[143] Human Rights First, "List of Public Congressional Recommendations for Global Magnitsky Sanctions", https://www.foreign.senate.gov/imo/media/doc/04-0319%20RM%20Rubio%20Letter%20to%20Pompeo%20Mnuchin%20Ross%20re%20Uighur%20detentions.pdf

[144] Paul Mozur, Jonah M. Kessel and Melissa Chan, "Made in China, Exported to the World: The Surveillance State", *New York Times*, 24 April 2019, https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html

[145] Lauly Li, Coco Liu and Cheng Ting-Fang, "China's 'Sharp Eyes' Offer Chance to Take Surveillance Industry Global", *Nikkei Asia*, 5 June 2019, https://asia.nikkei.com/Business/China-tech/China-s-sharp-eyes-offer-chance-to-take-surveillance-industry-global

[146] Aarti Nagral, "Dubai Crown Prince Reviews Smart Area Project That Will Use AI to Cut Crime", *Gulf Business*, 8 October 2018, https://gulfbusiness.com/dubai-crown-prince-reviews-smart-area-project-will-use-ai-cut-crime/

artificial intelligence surveillance program, Oyoon launched with the installation of thousands of CCTV cameras equipped with biometric surveillance capabilities across tourist destinations, traffic zones and public transit regions. As in China, the stated goal is to reduce crime: since the program's implementations, officials reported 319 arrests and cited a 99.5% decrease in unresolved and disturbing crimes in 2018 alone.[147]

Cautionary measures must, however, be taken when faced with these statistics. Much like Beijing, Dubai makes use of a charitable interpretation of the term 'criminals'; to include not only criminals like thieves and robbers but also political dissidents, human rights activists and journalists potentially threatening the monarchy.[148] With the UAE's highest rates of political prisoners per capita in the world,[149] legal acceptance of flogging and stoning practices, and a history of torture, the incorporation of technology may only serve to dramatically magnify such immoral state action.

Of specific note recently is the UAE's Project Raven, a secret hacking operation launched in 2009 under the guise of counterterrorism efforts. The project has been in part effective in achieving its aims: it has since helped the National Electric Security Authority (NESA) break up an ISIS network and aided in the investigation of potential assaults following an ISIS-claimed stabbing of a teacher in 2014.[150] However, the broad scope of 'criminals' has also resulted in Project Raven targeting many others on arguably unjustifiable terms. For example, Rori Donaghy, a British journalist who reported on and publicly lambasted the country's poor human rights records, found many of his networks hacked. To a more extreme extent, Ahmed Mansoor, a prominent activist and a critic of Emirati policy, was sentenced to prison for 10 years for sharing his views on Facebook and Twitter. Specifically, he was convicted of 'publish[ing] false information, rumours and lies about the UAE and promot[ing] sectarian feelings and hatred that would damage the UAE's social harmony and unity'.[151] Many others singled out include other journalists and dissidents, among them American citizens. Project Raven's precedent provides a strong warning of the prospective implications of Oyoon.

The UAE's success in these hacking operations and surveillance methods are in part due to resources provided for by the West. Many of Project Raven's capacities are taken from methods learned from the US intelligence community, the UAE having contracted with Baltimore-based cybersecurity firm, Cyberpoint.[152] After

---

[147] Ali Al Shouk, "How Dubai's AI Cameras Helped Arrest 319 Suspects Last Year", *Gulf News*, 18 March 2019, https://gulfnews.com/uae/how-dubais-ai-cameras-helped-arrest-319-suspects-last-year-1.62750675

[148] Freedom House, "Freedom on the Net 2018 – United Arab Emirates", https://freedomhouse.org/country/united-arab-emirates/freedom-world/2020

[149] Joe Odell, "How the UAE's Pro-democracy Movement Fell into a Death Spiral", *Middle East Eye*, 2 April 2018, https://www.middleeasteye.net/opinion/how-uaes-pro-democracy-movement-fell-death-spiral

[150] Christopher Bing and Joel Schectman, "Special Report: Inside the UAE's Secret Hacking Team of U.S. Mercenaries", *Reuters*, 30 January 2019, https://www.reuters.com/article/us-usa-spying-raven-specialreport/special-report-inside-the-uaes-secret-hacking-team-of-u-s-mercenaries-idUSKCN1PO19O

[151] Amnesty International, "UAE: Activist Ahmed Mansoor sentenced to 10 years in prison for social media posts", 31 May 2018, https://www.amnesty.org/en/latest/news/2018/05/uae-activist-ahmed-mansoor-sentenced-to-10-years-in-prison-for-social-media-posts/

[152] Christopher Bing and Joel Schectman, "Inside the Uae's Secret Hacking Team of American Mercenaries: Ex-NSA Operatives Reveal How They helped Spy on Targets for the Arab Monarchy — Dissidents, Rival Leaders and Journalists", *Reuters*, 30 January 2019,

National Security Agency (NSA), Cyberpoint was granted a license by the State Department in 2014 to provide sensitive defense technology and services to Dubai for the 'protection of UAE sovereignty'.[153] Despite express bans of targeting American citizens and companies, the methods have allowed non-American personnel on the project to hack into iPhones of activists, political leaders and American journalists alike. Further, Cyberpoint's successor as the primary cybersecurity contractor, UAE-based firm DarkMatter, was reported to have significantly invested in recruiting top-level talent from American companies such as Google, Qualcomm and McAfee.[154]

A Buzzfeed investigative report of procurement records revealed that Oyoon is also backed by global suppliers.[155] These suppliers include Canfield Scientific, Inc., a New Jersey-based biotech company specializing in 3D models; Nuance, a voice recognition company based in Massachusetts; and NEC, a Japanese company providing facial matching capabilities. Other companies with global reach are also setting their sights on the UAE as a viable market for their products, with Hikvision, Huawei and IBM marketing their biometric surveillance systems for use in the country.

There should be a US response to these UAE actions. For the protection of national security and the maintenance of democratic values, the United States should (1) sanction any commercial connections affiliated with Oyoon, as it did with China, and (2) negotiate qualifying terms for the future use of American-supplied tools, the two to be done concurrently. On the former, American companies wishing to contract products to Oyoon or Project Raven must first obtain government approval, as with Huawei and Hikvision. Ramifications of Project Raven have shown that such projects may pose grave threats to US national security, specifically in its targeting and hacking of Americans, and its violations of human rights. With this, the United States must tread carefully so as to not facilitate

American support of Project Raven's nefarious activities.

We should also consider potential repercussions should the United States completely block the UAE from purchasing American-made technology products. The Trump administration's restrictions on sales of products by US suppliers to Huawei could severely impact the bottom line of companies like Intel and Qualcomm, and a total prohibition might have the unintended consequence of inducing China to

[153] Ibid

[154] Jenna, McLaughlin, "Spies for Hire", *The Intercept*, 24 October 2016, https://theintercept.com/2016/10/24/darkmatter-united-arab-emirates-spies-for-hire/

[155] Megha Rajagopalan, "Facial Recognition Technology Is Facing A Huge Backlash In The US. But Some Of The World's Biggest Tech Companies Are Trying To Sell It In The Gulf", *BuzzFeed News*, 29 May 2019, https://www.buzzfeednews.com/article/meghara/dubai-facial-recognition-technology-ibm-huawei-hikvision

accelerate its own research into and development of the products.[156] This would only increase current tensions between the two superpowers. Pushback from the US blacklisting of Huawei might be a harbinger of similar headwinds for proposed restrictions on sales to the UAE. As a result, the United States must be mindful of the lessons learned, both about the impact on the US economy and of the stimulus to China's home-grown capabilities, as it prepares to implement similar restrictions

on sales to the UAE.

Technology has indeed played a role in elevating the power of autocrats, as it has in China and the UAE. To stem the rising tide of authoritarian rule, actions taken by the United States towards China need to be similarly applied to the UAE in order to conserve national security and democratic principles. However, restrictions or sanctions placed on the UAE need to be undertaken with care and forethought. Because the UAE is the United States' primary counterterrorism ally in the Middle East, US policy must allow for a future opening in the supply of American products. To that end, the United States must explicitly negotiate stricter terms of use for supplied American products while emphasizing the importance of maintaining a cooperative relationship between the two countries.

Adopting cyber security strategies that violate human rights

The use of loaded, imprecise language has had far-reaching consequences, as many governments are using vague internal and external threats as arguments to justify ever-greater investments in cyber arms and mass surveillance schemes, and ever-greater governmental control of the Internet and their own citizens. The sense of alarm embedded in cyber security narratives has clouded the need to objectively and evidentially substantiate the likelihood and nature of the dangers at hand. It has also given rise to the impression that all responses are appropriate and legitimate. For example, as we pointed out earlier, in many countries, both democratic and non-democratic, the threats posed to national security have long been used to justify extensive surveillance mechanisms, with more and more citizen data collected and easily accessed by state authorities. Other ominous 'security' measures include developing so-called 'Internet kill switches' (the notion of shutting down the Internet in order to protect it), restricting the use of encryption, implementing filtering and blocking mechanisms, and introducing real name policies. Such measures often pose threats to civil liberties, yet they tend to lack judicial oversight as well as public data upon which to judge their effectiveness (often because of claims that disclosure would impact security efforts). While it is not at all clear

[156] Lorand Laksai, "Why Blacklisting Huawei Could Backfire", *Foreign Affairs*, 19 June 2019, https://www.foreignaffairs.com/articles/china/2019-06-19/why-blacklisting-huawei-could-backfire

that they improve security, they frequently risk erasing the benefits the Internet brings.

'The same rights that people have offline must also be protected online' - this simple statement, adopted by a UN Human Rights Council Resolution on July 2, 2012, confirmed what had seemed obvious to human rights activists for many years.[157] It is extremely important, however, as it demonstrates government acceptance that there are clear international legal limits on the actions that they can legally take in the cyber domain. Laws and practices which interfere with human rights online are only legitimate to the extent to which they fall within the narrow constraints allowed under international human rights law. It is, therefore, necessary to revisit the cyber security agenda in light of human rights standards and values.

From a negative to a positive conception of cyber security

What, then, does a human rights approach to cyber security entail? First of all, such an approach puts the interests of citizens back at the center of any cyber security policy. States tend to view security in the negative sense as the mere absence of harm. As such, the sole aim of any security policy is to keep this harm at bay. Using this negative conception of security has led to policies and practices which disempower the people they seek to serve. What is more, those in power – in current discourses generally identified as governments or businesses – invariably benefit disproportionately in the process.

Debates around food and human security have amply illustrated, however, that security need not necessarily refer simply to the absence of harm. In a substantive sense, security is a positive concept: one that refers to a person's ability to gain access to a crucial resource and to use that resource according to their needs and preferences. A human rights approach to cyber security similarly foregrounds a positive understanding of security which focuses on people's capacity to act.

Where the Internet is concerned, security from a human rights perspective does not simply entail keeping people safe. Cyber security policies should not merely play a defensive role, but a facilitating role, by effectively putting the empowerment and well-being of people at their centre. What we are aiming for is for people to be able to be fearless, as long as they are respecting other people's human rights.

Ensuring 'solutions' do not become threats

Defined in this way, a human rights approach to cyber security reminds us that in order to assess the effectiveness of a cyber-security measure, it is essential to take into consideration not only the potential impact of the various threats to cyber security but also the proposed solutions. If a measure taken in the name of protecting people from harm undermines their human rights in such a way, and to such an extent that their ability to gain access to and use the Internet has been considerably impeded, it cannot be considered a reasonable security measure.

[157] UN Human Rights Council, "The Promotion, Protection and Enjoyment of Human Rights on the Internet" (A/HRC/20/L.13). New York, United Nations General Assembly, 16 Juy 2012, https://digitallibrary.un.org/record/845728?ln=en

Such an approach immediately makes clear why cyber surveillance has become such a contested topic around the world. Though cyber security and surveillance are often mentioned by governments as two sides of the same coin, as if one somehow necessarily requires the other, the relationship between the two is actually a deeply uneasy one. Surveillance frequently requires or implies an increase in vulnerability - for example when governments demand access to encryption or prescribe maximum levels of encryption. In the name of security, people are encouraged to give up the very tools – as well as agency – that allow them to protect themselves and to shape the Internet environment that they have defined for themselves as desirable. In most cases, this is without it being clear precisely which threats are being addressed; how effective the responses are in doing so; and what the cost-benefit analysis is from the perspective of Internet users. Surveillance measures that are currently in place in countries from India to the UK fundamentally undermine the fearlessness of their populations when they come online. In fact, in the case of South Korea's real name policy, the policy was in fact found to make people more insecure, as the collected data was exposed through several high-profile hacking attacks.[158]

Many people do accept that government agencies might need to engage in cyber surveillance of specific individuals for specific reasons. However, surveillance needs to be both necessary and proportionate to the threat. These conditions are frequently unfulfilled. Rather than supporting each other, cyber security and surveillance are frequently at odds. If we are to develop cyber security policies that fundamentally support human rights, it is essential that this be recognized and accounted for.

Applying a human rights approach to cyber security

International Legal Standards

Applying human rights law to cyber security debates, policies and practices will rely on all actors familiarising themselves with human rights standards and promoting them consistently. In recent years there have been a number of attempts to define exactly how international human rights standards apply to the Internet environment. The reports of the UN Special Rapporteur provide a good understanding of how freedom of expression applies. The 'International Principles on Communications Surveillance and Human Rights' (summarised in Annex I), describes the main principles of a human rights approach to cyber security as delineated by a group of civil society organizations,

[158] Freedom House, "South Korea Internet Freedom Report 2012", available at: http://www.freedomhouse.org/report/freedom-net/2012/south-korea

industry and international experts. Article 19's Johannesburg Principles on National Security provides principles for applying the legitimate aim of 'national security'.

Privacy and freedom of expression

Although other human rights (such as the right to peaceful assembly and association, the right to an effective remedy and the presumption of innocence) are also relevant, two human rights, in particular, will form the building blocks of rights-respecting approaches to cybersecurity. One is the right to privacy, or the right to keep one's data and communication away from the prying eyes of governments, businesses or other citizens. The right to privacy is a necessary component in the development of a citizen-centric security policy. However, it is not sufficient, as it does not exhaust the requirements for being secure online in the manner we defined above. For example, the right to privacy does not provide sufficient safeguards against content controls instituted by governments in the name of security policies at the locations where Internet cables enter a country. Privacy can be interfered with when a person is denied the confidentiality of their communications or the control over information about them. In the assessment of cyber security policies, equal stature should be given to the substantive enjoyment by all citizens of the right to freedom of expression. The other central right, freedom of expression, is interfered with when an action prevents someone from seeking, receiving or imparting any expression other than that which can be legitimately limited, and actions which 'chills', i.e. discourages or inhibits, that expression.

Both of these rights can, by law, be restricted under certain circumstances. However, interferences with freedom of expression will only be legitimate if they follow the tripartite cumulative test being provided by law which is clear and accessible to everyone, for one of the purposes outlined in article 19 (2) ICCPR,[159] necessary and the least restrictive means available to achieve that aim. Similarly, interferences with the right to privacy require that 'there must be a law that clearly outlines the conditions whereby individuals' right to privacy can be restricted under exceptional circumstances, and measures encroaching upon this right must be taken on the basis of a specific decision by a state authority expressly empowered by law to do so, usually the judiciary, for the purpose of protecting the rights of others, for example, to secure evidence to prevent the commission of a crime, and must respect the principle of proportionality.'[160] These terms and tests have been developed and elaborated on through case law and soft law standards. Any security measure that does not adhere to these strict criteria, while possibly increasing the security of the network, undermines the substantive security of the people. It undermines fearlessness.

[159] OHCHR "International Covenant of Civil and Political Rights", available at: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

[160] Supra note 8 at para 59.

corruption and scandal in high places. In the Internet age, however, the ability to communicate anonymously is increasingly under threat. In a growing number of countries, the use of mobile phones, Internet connections and even cyber cafes is possible only after users have registered and provided extensive documentation. In some countries, real-name identification systems for the use of services once a user is online have also been suggested or implemented. Increasingly, intelligence agencies seem to effectively be tracking the activities of a wide range of users online – either their own citizens or of citizens of other countries – without sufficient safeguards in place to protect users' rights to privacy or the presumption of innocence. In such circumstances, the ability to communicate anonymously is effectively destroyed, as is the presumption of innocence. As South Korea's Constitutional Court commented when assessing the constitutionality of the country's Internet Identity Verification Rule, systems that make it mandatory for users to provide identification, data treat 'all people as potential criminals'. The Court further observed that 'Anonymous speech on the Internet, rapidly spreading and reciprocal, allows people to overcome the economic or political hierarchy offline and therefore to form public opinions free from class, social status, age, and gender distinctions, which make governance more reflective of the opinions of people from diverse classes and thereby further promotes democracy. Therefore, anonymous speech on the Internet, though fraught with harmful side-effects, should be strongly protected in view of its constitutional values.' [161] Yet, surveillance measures in many countries continue to undermine anonymity online.

Public-private information sharing?

Such problems are compounded by the fact that many cyber security strategies create mechanisms to promote greater information sharing between private companies and government officials to allow for improved responses to cyber security threats. To an extent, this is an inevitable approach in a multi-stakeholder field where both actors hold parts of the information that is needed to successfully detect and counter threats. However, where close private-public relationships, including information-sharing, develop without adequate safeguards, this can easily lead to human rights violations. For example, in a recent long-running case in the US, it has been revealed that AT&T, a US telecommunications giant, shared enormous quantities of user data with the National Security Agency without any warrant. Many cyber security strategies mention the need to create such mechanisms but include no detail about what information will be shared, who will decide that the information is shared, what safeguards there are to prevent arbitrary or illegal sharing of information, how undue influence will be avoided, etc. It is important that any such mechanism is well defined and subjected to adequate scrutiny and safeguards.

Safeguards for 'metadata' versus actual content?

An additional problem is that many countries seek to apply lesser protections

[161] Quoted in 6 Park Kyung Sin, "Korean Internet Identity Verification Rule Struck Down Unconstitutional; 12 Highlights of the Judgment", *K.S. Park's Writings* (blog), 25 August 2012, http://blog.naver.com/kyungsinpark/110145810944.

for 'metadata' or communications data than they apply to the actual content of those communications. Communications data refers to, for example, the email address of a sender and recipient of an email, together with the date/time of the message, and the IP addresses of the computers used; or the logs of website addresses visited by a user. It does not include the actual content of the communication. In many countries, this distinction was developed in the offline world where limited information could be garnered from collecting the details of landlines phone calls or the addresses on envelopes. However, given the vast range of activities most Internet users use the Internet for and given the increased ability of the state to collect, store, cross-reference and use this data, it cannot be considered analogous with the same content in an offline world. In fact, it can be argued that metadata can reveal even more than the contents of the communication as it may reveal information that the individual did not realize they were sharing with anyone. The degree to which metadata is or is not different from content, and therefore deserving of different safeguards for access to this data by public authorities is an increasingly important legal question that human rights activists must engage with.

What constitutes valid online protest?

The Internet and digital communications are not only widely used to organise offline protests, the Internet is also a domain within which protests have been conducted. For example, hacktivists from the online activist group 'Anonymous' launched distributed denial of service attacks against Paypal, MasterCard and others who stopped servicing payments to Wikileaks in the aftermath of the 2010 release of the diplomatic cables. In January this year, following the suicide of Internet activist Aaron Swartz, Anonymous hackers hacked into the website of the US Department of Justice to protest against what it described as the harsh treatment of Swartz. The hackers defaced the Sentencing Commission site with an alternative video praising Swartz and denouncing the government.

At present, these is no clear definition of what constitutes legitimate protest in the online domain. In fact, the UK Cyber Security Strategy 2010 identifies politically-motivated hackers as one of the primary perpetrators of cyber security risks, without any discussion about whether such hacking may in certain circumstances constitute legitimate speech. This is particularly obvious when it comes to prosecution and sentencing patterns. For example, a number of hackers involved in the attacks against Paypal were given hefty prison sentences (including an 18-month sentence). This is a much more severe sentence than a protester in a traditional sit-in would have been likely to receive. Hacktivists are often lumped together with cyber criminals in cyber security strategies, but it is important to distinguish between crimes and actions which can be more accurately defined as an attempt to protest and effect change. By clubbing all hacktivists together with criminals, governments are undermining citizens' right to dissent.

Do we need demilitarization of the cyber security debate?

There are signs that some governments have invested in developing cyber arms and offensive cyber-attacks. These trends are extremely worrying from a human rights perspective: they are likely to lead to a curb on civil liberties as governments argue that curbs are necessary to promote security and that weapons' could be developed that cause real damage to the Internet architecture, preventing individuals from using it and gaining the benefits thereof. This is especially true in an interconnected ecosystem like the Internet where it is impossible to contain the impact of any so-called cyber war. There have been recent attempts to look at how humanitarian law applies to the online space, for example by the International Group of Experts convened by NATO (The Tallinn Manual). There is a need to also look at how human rights apply in situations of cyber war. However, perhaps even more important is for human rights activists to consider whether we need a cyber arms treaty or even a cyber demilitarisation movement. At present, not a single government has taken a leadership role in deescalating the cyber arms race, for example by indicating that they will not be the first to strike.

Cyber security and Internet governance

At the international level, concerns about cyber security feed into demands from states who want to assert their sovereignty over this new domain. In September 2011, for example, Russia, China, Uzbekistan and Tajikistan submitted a proposal to the United Nations General Assembly for an International Code of Conduct for the Information Society, calling for UN level action on the issue of cyber security. The preamble states that 'policy authority for Internet-related public issues is the sovereign right of the States'. This was also seen more recently at the World Conference on International Telecommunications in Dubai in December 2012, where governments from around the world met to renegotiate the International Telecommunications Regulations (ITRs). Many governments, particularly those from developing and transitional countries, sought to establish greater control over the Internet in Dubai by seeking to bring it firmly within the ambit of the ITRs. These attempts were often justified by security concerns and the inability of governments in question to address these adequately within current Internet governance arrangements.

A distributed-governance approach to cyber security

While cyber threats are often real, the current discourse is thus having a variety of negative impacts, moving the Internet governance agenda away from creating an accessible and enabling environment, towards finding new, and increasingly centralized, forms of command and control. A defining feature of the cyber security discourse is the notion of a powerful and benevolent state providing its citizens with security, as it did in the pre-Internet age. But this narrative sits uneasily with the reality of

the Internet's nature, which is a global network of information that is, to a large extent, in the hands of the private sector. Neither threats nor solutions are therefore as easily defined, located or circumscribed as they were in earlier eras. As Ron Deibert has pointed out, where state-based agencies are privileged as lead actors in securing this space, this can then 'create awkward privacy concerns in domestic settings while fuelling reciprocal suspicions on an international scale', not in the least because the actions of one state seem to affect the sovereignty of others.[162]

For this reason, Deibert proposes we move to a distributed approach to cyber security, which relies fundamentally on checks and balances among a variety of actors, both nationally and internationally, so as to avoid the emergence of 'unchecked and concentrated political power'. In a distributed approach, governance arrangements intentionally accord multiple actors specific roles and responsibilities in the cyber security arena but do so in such a way that no single actor is able to control this arena unless the others agree and collaborate. One of the strengths of such an approach is that it allows us to once again recognize the user as an important actor in this area. Indeed, as threats are fast-changing in the Internet environment, the best defence will often be having informed users who are able to make intelligent decisions; yet in the current governance arrangements, there is little space for this. In addition, by mandating multi-layers of checks and balances, such an approach would be more likely to support human rights.

To be effective, however, this approach also requires a strong commitment to mutual restraint as envisioned under international human rights law. This is required first and foremost on the part of states, who, at the moment, all too often engage in deliberate manipulation of security weaknesses and threats to their own ends. However, it is also needed on the part of Internet businesses, which possess large amounts of data on Internet users but often handle this in less than transparent ways. In both cases, all policies and practices should be brought in line with human rights standards, and oversight mechanisms should be established to consistently verify that this is indeed the case.

For current debates on global Internet governance and enhanced cooperation, this provides important pointers on the way forward. In the area of cyber security at least, what such conversations should focus on is not a renewal of government control traditional style, but the establishment of networks of governance actors and institutions, both domestically and internationally, who are linked in multiple ways and have a crucial stake in supporting and collaborating with each other.

In some cases, the formalization of the roles of different actors might require the establishment of new institutions and arrangements. However, such networks would also include existing multistakeholder mechanisms, such as ICANN, that already count as part of their responsibilities, particular aspects of cyber security, and could also integrate, to a greater extent than is currently the case, existing UN mechanisms. For example, the UN Human Rights Council could play a

[162] Ronald Deibert, "Dark Side of Cyberspace"

crucial role in conceptualizing and developing accountability mechanisms that respond appropriately to the peculiarities of the Internet while at the same time having the protection and promotion of human rights at their core. Each actor would play a crucial, well-defined yet circumscribed role, without being able to dominate the arena. If mutual restraint on the part of governments and businesses is crucial to enhancing cyber security for all, this should not simply be left to the good intentions of these actors. A distributed approach to cyber security is the way forward because it ensures that the need for restraint is embedded in governance arrangements and institutions.

Conclusion

There is an urgent need for a human rights approach to cyber security. Current cyber security debates suffer from a lack of definitional clarity that allows all initiatives in this area to be overtaken by a sense of crisis, whether or not such a sense is legitimate. In this atmosphere, insufficient efforts are made to establish the exact nature and seriousness of each threat and to investigate the cost of solutions offered and whether they actually counter the problem that they claim to address. In addition, the often problematic role of governments and businesses in contributing to insecurity is hidden from view. An important reason why this has been allowed to happen is because the approach taken to security is a negative one: security is defined as an absence of harm. In contrast, we propose a positive approach to security that puts people and their ability to be fearless online at the centre. Rather than the disempowering effect of current policies, such an approach would fundamentally empower people, including by substantively scaling back surveillance measures and returning to people their right and ability to protect themselves online.

At the heart of such an approach would be the extent to which cyber security measures respect and support the right to privacy and the right to freedom of expression. Though other human rights are relevant too, these are key rights to facilitate people's fearlessness online. By assessing contentious issues and their proposed resolutions against the extent to which they respect and support these rights, important progress could be made. Finally, this approach relies on governments and businesses agreeing to exercise mutual restraint. In order to institutionalize the principle of restraint, a distributed approach to Internet governance is required, which acknowledges and respects the role of a wide variety of actors and, through a system of checks and balances, ensures that none of these actors can control the field without the collaboration and agreement of the others. Such an approach would be more suited to the realities of the new environment that the Internet has brought about. It would also make it possible to shift the emphasis in cyber security state-centric approaches to ones that are people-centric.

ANNEX I.

International Principles on the Application of Human Rights to Communications Surveillance

In light of the proliferation of state surveillance of communications which does not adhere to international human rights law, a group of civil society groups, industry and international experts conducted a consultation about how existing human rights law applies to communications surveillance technologies and techniques. The result is the "International Principles on the Application of Human Rights to Communications Surveillance" released on 10 May 2013. Below is a summarised version of the principles (from http://www.necessaryandproportionate.net/):

• **Legality**: Any limitation to the right to privacy must be prescribed by law.

• **Legitimate Aim**: Laws should only permit surveillance to achieve a legitimate aim that constitutes an important legal interest that is necessary in a democratic society.

• **Necessity:** Laws must limit surveillance to that which is strictly and demonstrably necessary to achieve a legitimate aim.

• **Adequacy**: Any instance of communications surveillance authorized by law must be appropriate to fulfill the specific legitimate aim identified.

• **Proportionality**: decisions about surveillance must weigh the benefit sought to be achieved against the harm that would be caused to the individual's rights, and should consider the sensitivity of the information and the severity of the privacy infringement.

• **Competent Judicial Authority**: Determinations related to communications surveillance must be made by a competent judicial authority that is impartial and independent.

• **Due process**: Lawful procedures that govern any interference with human rights must be properly enumerated in law, consistently practiced, and available to the general public.

- **User notification**: Individuals should be notified of a decision authorising communications surveillance with enough time and information to appeal the decision.

- **Transparency**: States should be transparent about the use and scope of communications surveillance techniques and powers.

- **Public oversight**: States should establish independent oversight mechanisms to ensure transparency and accountability of communications surveillance.

- **Integrity of communications and systems**: States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for surveillance purposes.

- **Safeguards for international cooperation**: Where, under international agreements, the laws of more than one state could apply to communications surveillance, the standard with the higher level of protection for individuals should be applied.

- **Safeguards against illegitimate access**: States should enact legislation criminalizing illegal communications surveillance by public or private actors

ABOUT THE AUTHORS

Dr. Lora Pitman is a visiting research assistant professor in cybersecurity at Old Dominion University. She holds a Ph.D. in international studies from Old Dominion University, a Master's in Humanities from the same institution, and a Master's in Law from Sofia University, Bulgaria. She has published multiple peer-reviewed articles with a focus on international security and cybersecurity. Her publications appear in International Journal of Cyber Criminology, International Journal of Intelligence & Cybercrime, International Journal of Criminal Justice Sciences, Journal of Criminal Justice Studies, Politikon. She is also a co-editor of the NATO-issued volume Advances in Defence Analysis, Concept Development and

Dr. Metodi Hadji-Janev, (Ph.D.) is an associate professor of international law at the Law Faculty, University Goce Delcev Shtip and an adjunct faculty member at Ira A. Fulton School of Engineering, Arizona State University, ASU, USA. He holds MA and Ph.D. degrees in international law from the Law Faculty "Justinian-I" in Skopje, R. N. Macedonia and is a graduate of US Air Command and Staff College, Maxwell, Alabama, where he earned the title of 'Cyber warrior'. D-r Hadji-Janev's current work focuses on legal and strategic aspects (the governance and human rights perspectives) of countering cyber and hybrid-based threats (including an academic and professional focus on AI application and developments) while building social resilience.

Dr.Alexandros Sarris is a senior lecturer in international law at Erasmus University College in Rotterdam, The Netherlands. Alexandros has been trained in Europe and the United States in international law, international negotiations and international dispute settlement with a special focus on international conflicts that include among others natural resources, state sovereignty, responsibility of states, and the implementation of international agreements of all kinds.

Alexandru Georgescu is an expert (ranked scientific researcher) with the department for cybersecurity and critical infrastructure protection of the National Institute for Research and Development in Informatics ICI Bucharest. He is actively involved in advancing critical infrastructure protection and resilience issues through cooperation at the international level and has worked on international projects for the European Space Agency and others. Since 2019, he is a moderator of the Working Group on the Protection of Defence-related Critical Energy Infrastructures within the Consultation Forum on Sustainable Energy in Defence and Security Sectors organized by the European Defence Agency.

TACTICS INSTITUTE
For Security & Counter Terrorism