James Shires

Digital transformation and its implications for cyber security in the MENA region.

I. Introduction

Diplomats, like everyone else, move with the technological times. Formal invitations arrive by email, international treaty negotiations revolve around tracked changes documents in Microsoft Word, and last-minute negotiating offers and counteroffers circulate by WhatsApp or Signal. Such "cyber-diplomacy" or "digital diplomacy" highlights the significant influence of digital transformation on this notably elaborate and ritualised sphere of political activity. But diplomacy not only adjusts to incorporate new digital technologies and practices; it must also address new threats stemming from those technologies. At least since the first United Nations (UN) resolution on "developments in the field of information and communications in the context of international security" in 1998, the narrower field of cybersecurity diplomacy has become increasingly central to traditional diplomatic concerns of war, peace, and interstate relations. It has also posed new challenges to formerly state-centric models of diplomacy, as multinational technology companies and other non-state actors exert diplomatic power – think only of the famous (or infamous) "Public Library of US Diplomacy" published online by Wikileaks in 2010.

These Wikileaks documents were one of the many domestic and international triggers for the protests, revolutions and uprisings across the Middle East and North Africa (MENA) region known as the Arab Spring, as they revealed the extent to which authoritarian regimes had siphoned off state funds for personal enrichment.[1] However, cybersecurity diplomacy has taken longer to develop in the region, despite key junctures like the hosting of the inaugural World Summit on Information Society in Tunis in 2005, or a notoriously divisive World Congress on Information Technologies in Dubai in 2012.[2] It is only in the last five years that we have seen diverse and substantial efforts by states and non-state actors in the region alike to develop cybersecurity diplomacy capacity and bring it to bear on regional and global political issues. This article traces these developments, asking: how has cybersecurity diplomacy emerged in the Middle East?

The article argues that cybersecurity diplomacy provides Middle East states, primarily those of the Gulf Cooperation Council, with an additional platform to exert influence and project power on the international stage. But it also raises new questions about regional political alliances and organisations, with "Arab" cybersecurity initiatives juxtaposed against cybersecurity relationships across former geopolitical divides, such as the 2020 Abraham Accords. The article concludes with a reflection on the weaknesses of cybersecurity diplomacy in the region, including its relative irrelevance to regional conflicts.

II. The Middle East in global cybersecurity diplomacy

Global cybersecurity diplomacy is in flux. The current cybersecurity process in the UN 1st Committee, an Open-Ended Working Group (OEWG) led by Singapore, is under pressure to deliver tangible results in a tight timeline after previous iterations merely maintained

[1] Bachrach, *WIKIHISTORY: Did the Leaks Inspire the Arab Spring?*, 2011.
[2] Shires, *The Politics of Cybersecurity in the Middle East*, 2022.

momentum. The OEWG is supposed to transition to a Programme of Action in 2025, although the latter's mandate and scope remain unclear. These processes may be superseded by a Global Digital Compact, scheduled for unveiling at the UN Summit for the Future at the end of 2024, which addresses many of the same issues in addition to Artificial Intelligence (AI) and other emerging technologies. At the same time, in the UN 3rd Committee, an Ad Hoc Committee (AHC) to agree a global cybercrime convention appears to be imploding, with long-running divisions between democratic and open approaches to internet governance and more authoritarian stances – present in all these venues – showing no sign of alleviating sufficiently to reach agreement.[3]

Middle East states contribute vocally to all these processes. Iran, along with Russia and China (and Syria), has been a central proponent of more state-centred, authoritarian perspectives for decades. Egypt occupies a split role, a longstanding champion for less developed states across Africa and a familiar interlocutor for European and American diplomats, but with a growing closeness to the authoritarian approaches above. The Gulf states advocate for restrictive cybercrime measures while also looking to leverage their financial power to shape more inclusive conversations. For example, the UN Internet Governance Forum (IGF), the preeminent multistakeholder internet governance meeting for over 18 years, will convene in Riyadh in December 2024. The nomination of Saudi Arabia as the IGF's latest rotating location was highly controversial, with 88 civil society organisations worldwide signing a joint letter to the UN Secretary General calling on him to reverse this decision due to Saudi Arabia's history of human rights violations and internet censorship.[4]

The most pertinent global body for cybersecurity diplomacy in the Middle East, however, is the International Telecommunications Union (ITU). The ITU operates a Global Cybersecurity Index (GCI) which ranks all states' cybersecurity capacity, based on answers to a 30-page questionnaire submitted by relevant government agencies. The fourth GCI was published in 2020, with the next version due later this year. In the 2020 edition, Saudi Arabia came joint-second worldwide, with the United Arab Emirates joint-fifth. In the Arab region, Oman, Egypt and Qatar also scored higher than 90 points out of 100. The GCI is important not because of the robustness of its results – indeed, the questionnaire allows room for countries to maximise policy commitments rather than practical action – but because it is a highly visible and simple way to compare neighbours. Many cybersecurity agencies in the Middle East, especially in the Gulf, have included improvement in the GCI index as a key performance indicator, meaning that these states are much more oriented towards the ITU as a cybersecurity locus than they are the other UN processes.

In contrast, Middle East states have been far less prevalent in global multistakeholder cybersecurity initiatives over the past few years. Only five Middle East states signed the Paris Call for Trust and Security in Cyberspace, launched by the Paris Peace Forum in 2018 (UAE, Kuwait, Lebanon, Qatar and Tunisia). The 2024 UK-France Pall Mall Process on commercial cyber intrusion capabilities had the GCC in attendance as an organisation, with Saudi Arabia and the UAE individually also reportedly supportive, despite their extensively-reported reliance on such capabilities for surveillance and repression.[5] This relative lack of Middle East presence is due partly to the low priority such

[3] Kazakova, Ittelson and Kovač, *Decision postponed on the Cybercrime Convention*, 2024.
[4] Access Now, *Joint Statement: Internet Governance Forum must reverse decision to make Saudi Arabia its next host*, 2023.
[5] Herpig and Paulus, *The Pall Mall Process on Cyber Intrusion Capabilities*, 2024.

initiatives receive in a government-dominated policy landscape, as well as discomfort within those initiatives in welcoming authoritarian states (like the IGF above). Where multi-stakeholder cybersecurity collaboration is less politicised, some Middle East states do contribute. Egypt, Jordan, the UAE and Israel all participate in the International Counter Ransomware Initiative (CRI), with the UAE and Israel jointly contributing an information sharing platform developed with Microsoft to the CRI.[6]

Overall, Middle East states are starting to contribute more centrally to global cyber-security diplomacy, led by Saudi Arabia and the UAE. This does not, however, mean that cyberecurity diplomatic processes themselves will run more smoothly, given the balancing act these states strike between Western security alliances and authoritarian internet instincts. The ability of especially these two states to host – and financially support – major international conferences means that they are likely to be a regular presence in the cybersecurity diplomatic scene in the near future. Whether this convening power translates into more substantive influence over agendas and outcomes, however, remains an open question.

III. Regional cybersecurity diplomacy

The multilateral organizations above have regional offshoots focusing on the Middle East, which have also developed substantial cybersecurity activities over the past decade. The Arab IGF has waxed and waned since its creation in 2012, with the most recent in Lebanon in 2021 as part of a broader Digital Cooperation and Development Forum, hosted by the UN Economic and Social Commission for Western Asia (ESCWA), based in Beirut. ESCWA has long sought to improve cyber-security awareness and governance among Middle East governments, publishing a "regional roadmap" for internet governance in 2010 that was soon overtaken by the Arab Spring events.[7] However, cybersecurity – as an issue closely connected to national and international security – is technically outside ESCWA's remit, meaning that many events, such as a September 2023 workshop on "building trust in digital public services" at which I spoke, must tackle cybersecurity issues in all but name.

ESCWA's main partners in this workshop, the Arab Information and Communication Technologies Organization, based in Tunisia, and the Arab chapters of the Internet Society, a global multistakeholder organisation, have each developed their own regional initiatives. In March 2020, the Internet Society released guidelines for securing internet infrastructure addressed specifically to Arab states, seeking to build support for its technical measures for routing security.[8] In January 2024, the ICT Ministers' Council of the Arab League approved an Arab Cybersecurity Strategy following the publication of similar national strategies in the region (and, in some cases, multiple iterations).[9] A separate Arab League Council of Ministers for cybersecurity was established in September 2023, championed by Saudi Arabia, meaning that over the coming years the usually lethargic League may devote greater attention and resources to the issue.[10] This follows the creation of a similar Ministerial Committee for cyber-security in the GCC, which met for a second time in November 2023.[11]

---

[6] Israel National Cyber Directorate, *Press Release*, 2023.
[7] UN ESCWA, *Arab regional roadmap for Internet governance: framework, principles and objectives*, 2010.
[8] Internet Society, *Internet infrastructure Guidelines for Arab States*, 2020.
[9] AICTO, *Arab ICT Ministers' Council approves the Arab Cybersecurity Strategy*, 2024. For national cyber-security strategies, see Shires, *The Politics of Cybersecurity in the Middle East*, 2021.
[10] Almutairi, *Arab League announces establishment of Council of Ministers for Cybersecurity*, 2023.
[11] Gulf Cooperation Council, *Press Release*, 2023.

ESCWA also partnered with the ITU for its 2023 workshop, which has a far more extensive history of developing regional cybersecurity efforts. The ITU established an Arab Region Cybersecurity Centre (ARCC) in Oman in 2013, which has conducted many joint cyber drills with other countries and holds an annual regional cybersecurity conference, as well as leading the way in cybersecurity awareness campaigns that have now been taken up by other states, such as the UAE. The ARCC both benefits and suffers from its location in Oman. While lacking the financial resources of its richer neighbours, the ARCC is nonetheless able to establish connections between technical practitioners in more diplomatically difficult states, such as Iran, and via broader networks such as the Organization of Islamic Cooperation and a global network of computer incident response teams, FIRST (which includes nearly all Middle East states as members, and regularly offers training in the region).

More recently, Saudi Arabia has launched several other initiatives that recentre the locus of cybersecurity diplomacy towards the kingdom. In 2020, it led the creation of the Digital Cooperation Organization, an ostensibly global multilateral organisation with half its member states in the Middle East – the current presidency is held by Bahrain. Saudi Arabia's annual Global Cybersecurity Forum, also inaugurated in 2020, has dominated the regional cybersecurity landscape and attracted businesses and politicians from outside the region, even during its Western diplomatic isolation after the killing of Jamal Khashoggi in 2018 (in which Israeli spyware was a contributing factor).[12] In 2023, the GCF launched a stand-alone Institute to continue its activities outside the annual event. Added to the UAE's annual GISEC conference and Bahrain's Arab International Cybersecurity Summit, the calendar is now full of competing events, all seeking to promote their state sponsors as the most advanced in the region. The Gulf countries all compete at a commercial level too, aiming to attract individuals with cybersecurity skills – offensive and defensive – that are in short supply worldwide.

This healthy competition extends beyond summit diplomacy into other areas of cybersecurity governance. A regional trend for centralisation of national cybersecurity policy and decision-making into a single authority or centre – each with its own international cooperation department – not only follows best practice worldwide, but also illustrates the integral role non-diplomats play in cybersecurity diplomacy. These organisations indirectly affect cybersecurity diplomacy by setting national standards, regulations and controls that are then adopted by businesses and adapted by other states. More generally, cybersecurity capacity-building – the subject of much attention at the UN OEWG – is now garnering greater attention in the Middle East, with states like Saudi Arabia and the UAE looking to increase regional influence by offering training, equipment and collaboration to other states in the region and beyond. Such capacity-building efforts are promising, but with several obstacles: they run not only the risks of duplication and inefficiency, but also the misuse or abuse of capabilities to increase cyber insecurity.

IV. The future of regional cybersecurity diplomacy

While this article has traced the rapid rise of cybersecurity diplomacy as a national and regional priority, much remains to be done. Most significantly, cybersecurity diplomacy has had little impact on devastating regional conflicts from Libya to Yemen, and from Syria to Gaza. These enduring or recurring wars seem to take place on a different plane to cybersecurity diplomacy, where conversa-

[12] Kirchgaessner, *Saudis behind NSO spyware attack on Jamal Khashoggi's family, leak suggests*, 2021.

tions revolve around shared threats and joint economic opportunities. The disconnect is self-reinforcing: such countries suffer from a lack or destruction of digital infrastructure and investment due to conflict, which then makes them less able to participate or contribute to regional diplomatic activities, which then exclude them further and deepen digital divides.

Indeed, this disconnect can be convenient or even deliberate. The 2020 Abraham Accords normalising relations between Israel and four Arab states, led by the UAE, included cybersecurity and digital technologies as a key plank of cooperation – especially regarding shared cyber threats from Iran. Through this agreement, the UAE benefited from Israel's world-leading cybersecurity technologies and Israel gained a new (or rather, more overt) market for its commercial cybersecurity sales, while the relationship between the Israeli cybersecurity sector, its military underpinnings, and surveillance and repression in the West Bank and Gaza were almost entirely obscured. To truly contribute to regional peace and stability, cybersecurity diplomacy in the Middle East must develop further, transitioning from a marker of digital inequality to an ameliorating factor, and helping to solve rather than avoid regional escalation and conflict.

Reference list

Access Now, "Joint Statement: Internet Governance Forum must reverse decision to make Saudi Arabia its next host," October 12, 2023, https://tinyurl.com/4cekhzrx.

Arab Information and Communication Technologies Organization (AICTO), "Arab ICT Ministers' Council approves the Arab Cybersecurity Strategy," January 20, 2024, https://tinyurl.com/mvect3p9.

Almutairi, Dhai, "Arab League announces establishment of Council of Ministers for Cybersecurity," *Arab News*, September 11, 2023, https://tinyurl.com/36f8wvkf.

Bachrach, Judy, "Wikihistory: Did the Leaks Inspire the Arab Spring?," *World Affairs* 174 (2: 2011): 35-44.

Gulf Cooperation Council, "Press Release," November 9, 2023, https://tinyurl.com/28z24nvf.

Herpig, Sven, and Alexandra Paulus, "The Pall Mall Process on Cyber Intrusion Capabilities," *Lawfare*, March 19, 2024, https://tinyurl.com/3rtnuj4v.

Internet Society, "Internet infrastructure Guidelines for Arab States," May 18, 2020, https://tinyurl.com/277ts3tz.

Israel National Cyber Directorate, "Press Release," June 28, 2023, https://tinyurl.com/5x96bhk7.

Kazakova, Anastasia, Pavlina Ittelson and Bojana Kovač, "Decision postponed on the Cybercrime Convention," *DigWatch*, March 7, 2024, https://tinyurl.com/b884p589.

Kirchgaessner, Stephanie, "Saudis behind NSO spyware attack on Jamal Khashoggi's family, leak suggests," *The Guardian*, July 18, 2021, https://tinyurl.com/rjr4d5dk.

Shires, James, *The Politics of Cybersecurity in the Middle East* (Oxford: Oxford University Press, 2022).

United Nations Economic and Social Commission for Western Asia (ESCWA), "Arab regional roadmap for Internet governance: framework, principles and objectives", January 2010, https://tinyurl.com/479mep6m.

All internet sources were accessed and verified on 25 March 2024.