مركز البيان للدراسات والتخطيط
Al-Bayan Center for Planning and Studies

Constructing an Interinstitutional and interministerial effort on Cyber Security in Iraq

Shubbar, Hashim

Al-Bayan Center Studies Series

About

Al-Bayan Center for Planning and Studies is an independent, nonprofit think tank based in Baghdad, Iraq. Its primary mission is to offer an authentic perspective on public and foreign policy issues related to Iraq and the region.

Al-Bayan Center pursues its vision by conducting independent analysis, as well as proposing workable solutions for complex issues that concern policymakers and academics.

Copyright © 2022

www.bayancenter.org
info@bayancenter.org
Since 2014

Constructing an Interinstitutional and interministerial effort on Cyber Security in Iraq

Shubbar, Hashim*

Introduction

In 2017 the office of the National Security Advisor published the Iraqi Cybersecurity Strategy (ICS), marking the first substantial and public effort by the Iraqi state to analyse the deficiencies in national cyber policy; drawing a road map for the construction of a cyber suprastructure for the nation to put Iraq on par with its international counterparts and allies.[1] The first of its kind, the ICS accurately diagnosed the gaps in Iraq's cyber policies as structural weaknesses related to human neglect, unexamined measures and deprioritization of the cyber domain. Consequently, the strategy lays out an implementation agenda based on one-, three- and five-year fulfilment objectives ranging from the establishment of a federal cyber agency and the drafting of laws relating to the cyber space to the "creation of a cyber security culture" and university degrees in cyber security.[2]

While the publication of such a document should be applauded as a display of the increasing prioritisation of the cyber domain, the ICS of 2017 is nonetheless acutely flawed and has largely failed to induce the application of the framework it proposes. The Cybersecurity Strategy published was largely theoretical, detailing the general threats faced by private and public actors in cyberspace rather than focusing on the nature of the cyber threats Iraq faces in particular.[3] Consequently, the strategy did not attempt to provide what can be considered a concrete analysis or schema for the classification of critical infrastructure which is or could be the subject of frequent targeting. Moreover, the document failed to outline which government entity or institution would be responsible for the implementation of its recommendations, plans or objectives; providing no detailed

1.National Security Advisor "Iraqi Cybersecurity Strategy 2017" International Telecommunications Union. 2017

2. Ibid

3. Asmaa Khalid Jarjees Al-Tae, Hameeda Abdul-Hussain Al-Dhalimi, Adnan Kadhum Jabbar Al- Shaibani "Relationship of Cybersecurity and the National Security of the Country: Iraq Case Study." Systematic Reviews in Pharmacy. December 2020, p. 474

*Currently a Masters Student of International Security, Global Risks and the Middle East at Paris Institute of Political Studies, Hashim Shubbar is Defence and Security Analyst focused on Iraq and the wider Arabian Gulf region.

strategic programs nor periods of implementation for the policies mentioned. Ergo, none of the objectives, policies or reforms suggested and proposed have seen any real progress in terms of their realisation.

Taking into account the general groundwork laid down by the 2017 ICS, its shortcomings as well as the prevailing risks and threats in the cyber domain in Iraq, and the international guiding principles around cybersecurity, the Iraqi National Security Advisory, the Iraqi intelligence services and the Iraqi government should take into account the following recommendations:

1. Working with international partners — both private and public — to launch Iraq's own communications satellite to create the necessary bedrock infrastructure for an integrated information security system,

2. Charting a legislative, legal, and judicial ecosystem around the cyber domain which provides national standards and regulations for cybersecurity in both the private and public sectors, creating an enabling legal environment for enterprise and pricing an ecology for the persecution of cybercrime while ensuring civil liberties,

3. Establishing a dedicated national cyber agency under which cyber policy is implemented, responsible for cyber education and awareness, information security and the defence of the Iraqi national cyber space,

4. Entering into multinational treaties and agreements relating to cybersecurity as crucial mechanisms for codifying norms and behaviours while entering into bilateral treaties and agreements which stipulate both information sharing and capacity development,

5. Incentivising third country private sector expertise to install in Iraq to fill the current gap in technical expertise and professionals, providing a base upon which Iraqi human capital can be nurtured, developed, and encouraged in the long term.

These recommendations were formulated through analysis and study of the current architecture of Iraqi cyber policy and the state of its communications infrastructure as explored thereafter in this brief, as well as the consultations of the conduct of more cyber advanced nations and the guidance provided by transnational communications and cyber bodies.

Observations

Iraq has been able to make a surprisingly strong entry into the cyber space after 2003 and the end of the sanctions-imposed technological isolation of the 1990s. As of 2017, approximately 20 million Iraqi residents — around half the population — are connected

to mobile internet service lines, with a similar percentage having access to the internet in their homes.[4] However, the long term political instability and security volatility of the country has largely deprioritized the development of mature state mechanisms, policy and infrastructure around this growing cyber domain in the country, thus this growth has exposed, to a large degree, Iraq's weaknesses with regards to cyber and information security.

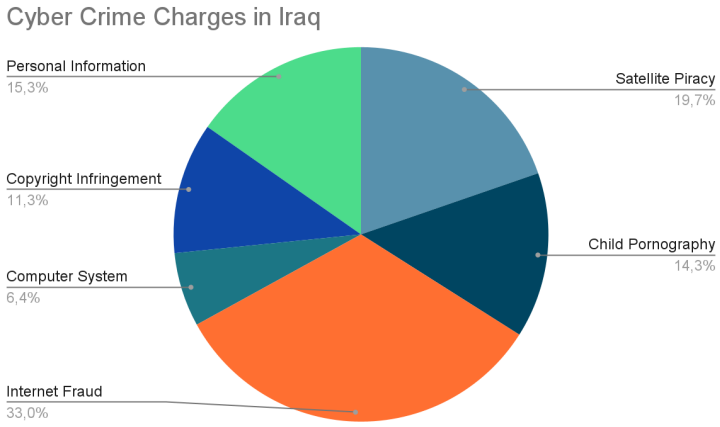
The Iraqi state and the majority of its institutions continue to rely on satellite providers beyond the country's territory in order to process information. This reliance amounts to a critical breach in Iraqi information security as information necessarily must be directed through the servers of third countries.[5] In practice, as long as this reliance on extraterritorial servers and satellites is maintained, the nation is incapable of building a truly integrated security system. As recently as September 2021, the government and the ministry of communications had announced plans for the construction and launch of Iraq's first communications satellite. However, the project remains in the bidding phase, as the government continues to look for foreign partnerships.[6]

The internet and cyber domain have also largely matured with no direction or influence from the state as Iraq continues to lack any judicial or regulatory framework for cyberspace. Iraq has no data protection law, while outdated and underdeveloped privacy legislation is largely retroactively applied to the internet. The Iraqi judiciary further lacks any specific legislation on cybercrime, meaning that the antiquated Iraqi Civil Code of 1951 and the Penal Code of 1969 is used with regards to cybercrimes.[7] This absence of a legal ecology around cyberspace has complicated the provision of comprehensive cybersecurity for both state institutions and businesses, while it has made the prosecution of the new and growing phenomena of cyber criminality increasingly difficult.[8]

As per the closed 2013 data provided by the government to Sattar J. Aboud in 2014, the vast majority of cybercrime in Iraq is carried out through social media platforms and particularly through Facebook:

4. Asmaa Khalid Jarjees Al-Tae, Hameeda Abdul-Hussain Al-Dhalimi, Adnan Kadhum Jabbar Al- Shaibani "Relationship of Cybersecurity and the National Security of the Country: Iraq Case Study." Systematic Reviews in Pharmacy. December 2020, p. 473
5. Ali Ziad al-Ali "The Hidden Threats to Iraq's National Security." Al-Bayan Center for Planning and Studies. July 2018
6. Mina Aldroubi "Iraq unveils plan to build and launch satellite" The National News. September 2021
7. Aro Omar "Law Update: Cybercrime Legislation in Iraq." Al Tamimi & Co. September 2017
8. Ibid

Figure 1. "Cyber Crimes in Iraq 2013"



Data from Sattar J. Aboud "Cyber Crime in Iraq." International Journal of Scientific & Engineering Research. March 2014

This data represents only a fraction of the likely occurrences of cyber criminality, as many of the crimes further include blackmail of a sexual nature and illicit substance sales both of which carry social stigma and repercussions which reduce citizen willingness to report such incidents to authorities.[9] 2019 saw an attempt by parliament to introduce a cyber criminality bill in the midst of some of the most violent protests in the country's history. These efforts were largely deemed by human rights organisations to be incredibly repressive and rather politically motivated rather than an attempt to introduce genuine legislative reform with regards to the cyber domain.[10] This politicisation of laws around cyber security could have long term implications on the trust both internal and external actors have in the good faith of the Iraqi government with regards to cybersecurity. As much as 70 percent of those polled by the UN expressed strong approval for tighter regulations on privacy, consumer protection and cybercrime in Iraq.[11] The public's participation and endorsement of such legislation is necessary if the goal of achieving a 'culture of cybersecurity' is to be achieved in the country.

9. Sattar J. Aboud "Cyber Crime in Iraq." International Journal of Scientific & Engineering Research. March 2014
10.Kristen Sibbald "Iraq Parliament Suspends Draconian Cybercrimes Bill" Human Rights Watch. May 2021
11. "Iraq sets sights on e-commerce opportunities" Conférence des Nations unies sur le commerce et le développement. July 2019

Iraqi cyber security vulnerabilities due to the aforementioned structural vulnerabilities extended to the state and its institutions. The Digital Centre in Iraq has reported that the quasi-majority of websites of government ministries do not meet basic ITU security standards and thus are easily penetrable.[12] This possibility was released in 2011 when several attacks were launched against the informational and data infrastructure of key government institutions — most notably the Iraqi parliament. The state was obliged to pay the undisclosed ransom figure to the hackers in order for the state's data to be released. The security institutions of the state at the time were unable to identify the culprit of the attack due to the lack of technical expertise; broadly narrowing it down to a foreign source.[13] More recently, Daesh [ISIS] was capable of using cyberwarfare against the contingents of the Iraqi state and Iraqi state institutions.[14] This campaign waged by such an existential threat to the state undoubtedly had a direct impact on inspiring the security establishment in the country to make cybersecurity considerations, resulting in the 2017 ICS.

The security apparatus and the relevant ministries have indeed slowly begun to incorporate, in one form or another, some cyber capabilities. However, these efforts are not centralised or coordinated by a specialised institution, and thus the resulting configuration is a plurality of teams and departments tucked into multiple civil and military government agencies. Consequently, both the coordinating and professional cooperation of these pre-existing efforts is diminutive.[15] A prime example of these institutional issues is the integration of the Iraqi national CERT team into the office of the National Security Advisor. The Iraqi NSA is one of the most powerful positions in the security establishment and is responsible for everything from coordination of civil military operations outside of Iraqi territory to the investigation of the recent assassination attempt of the Prime Minister. Thus, the CERT team, working under his office is not being utilised to its full capacities in terms of protecting private and public sector institutions and their services; rather they are one of the many instruments the NSA maintains in order to fulfil particular duties.[16]

12. Asmaa Khalid Jarjees Al-Tae, Hameeda Abdul-Hussain Al-Dhalimi, Adnan Kadhum Jabbar Al- Shaibani "Relationship of Cybersecurity and the National Security of the Country: Iraq Case Study." Systematic Reviews in Pharmacy. December 2020, p 473
13. "Homeland Security Did Not Fulfill the National Cybersecurity Strategy of 2017" al-Hurra Iraq. June 2021
14. Asmaa Khalid Jarjees Al-Tae, Hameeda Abdul-Hussain Al-Dhalimi, Adnan Kadhum Jabbar Al- Shaibani "Relationship of Cybersecurity and the National Security of the Country: Iraq Case Study." Systematic Reviews in Pharmacy. December 2020, p 473
15. Ibid
16. Bassem Ali Khreisan "Cyber security in Iraq: a reading in the Global Cybersecurity Index 2020." Al-Bayan Center for Planning and Studies. July 2021, p.

Recommendations

The past 18 years of instability and political violence in Iraq has deprioritized the regulation of, and government engagement with, the cyber domain. However, as the country forges into the third decade of this century, the sovereignty of its cyberspace and cybersecurity are becoming an increasingly important factor in ensuring the desired prosperity and stability. The ITU's Cyber Security Index gives Iraq an overall score of 20.71, ranking in the middle range in comparison to other countries in the region.[17] Iraq, as the Arab World's 4th largest economy, and 6th largest in the region, is absolutely capable of building an integrated, well-regulated and highly effective cybersecurity ecosystem. Looking at the ITU's recommendations and contrasting them with the reality of the current architecture and state of cybersecurity in Iraq, a clear roadmap can be drawn for the state to adequately advance its capabilities, defence, and sovereignty.

The launch and operationality of the planned communications satellite must be prioritised in the short term in order to provide the Iraqi state with a base upon which the country's cyber sovereignty can be constructed; Iraq should not be dependent upon other nations for the processing, storage and transfer of its information if it hopes to seriously insure a high degree of information security. Even such an infrastructural effort will require the creation of the necessary legal and regulatory frameworks as well as an organisational structure to back them.

A dedicated legislative and juridical ecology around cybersecurity, cyber criminality and the cyber domain is also a top priority. Iraq's cyber criminality concerns will only continue to grow as larger percentages of the country continue to gain access to the web. The outdated Iraqi penal and civil codes cannot serve as the basis for prosecution of cybercrimes. It is vital that a whitebook of cyber security laws is introduced in a manner which maintains civil liberties and the confidence of the Iraqi public and business circles; taking the EU's legislation as a workable example of inspiration for the needed data protection, and privacy legislation while looking at Iraq's neighbourhood for examples of successful cyber criminality lawmaking. Iraq's legislation on cyber must further include regulations and standards upon which both the public and private sector can rely on. A major request by the private cyber security market in Iraq has been the deployment of a minimum standard — at least in key sectors such as healthcare, banking and telecommunications — whereby cybersecurity procedures can be standardised and thus better catered to.[18] These cyber infrastructures, laws and regulations should be enforced, organised and coordinated through a dedicated and centralised cyber government agency. It is important to note that inspiration for legislation from jurisdictions like the European Union must also take

17. "Global Cybersecurity Index 2020" International Telecommunications Union. 2021
18. Farook Al-Jibouri "Iraq Cyber Security Overview." Cyber Code Technologies FZE. December 2016

into account the failure points of such legislation models. The complexity of European legislation, for example, has the tendency to increase operational costs. An exhaustive study of both successes and failures experienced by other countries and jurisdictions is a relatively costless effort which would enable the Iraqi judiciary to bring forth legislation which is both up to date and adapted to its particular context and concerns.

The current devolution of Iraq's cyber security capabilities, teams and professionals does not enable the state to create a coordinated effort vis-a-vis its cyber domain, nor implement the strategies and goals it has for said domain. The Iraqi national CERT should be transferred to this agency, while several other response teams should be created to manage highly critical domains such as commerce, banking and healthcare. Moreover, this agency should be responsible for the cyber security advocacy in the country, similar to the function and structure of France's ANSSI. This sort of advocacy can take multiple forms, from advertisements raising awareness on national television to partnerships with universities and other formal institutes of education.

Furthermore, Iraq needs to emphasise both bilateral and multinational agreements with regards to cyberspace. The ITU understands bilateral agreements to be a driver for capacity development, of which Iraq is desperately in need. Moreover, the creation and codification of international norms and behaviours would better enable Iraq in combating cyber threats as aggression at the international level would be both discouraged and shunned.[19] Finally, Iraq needs to increase its investment in its cyber strategy and cyber policies. Neighbouring Iran, with a GDP per capita half that of Iraq's, has allocated 1 billion annually to its cyber security and cyber strategies, a budget which dwarf's Iraq's cyber allocation.[20] Iraq must actively invest and incentivise private sector actors both at home and abroad to install in Iraq and develop the necessary expertise and culture around the cyber space needed for the development of sectors such as e-commerce which the Iraqi government has outlined as a goal for the country's economic maturation.[21] A cultivated and complete cyber security policy, which is actively and annually updated and adjusted promises to not only increase the security of Iraq, its government and its population in cyberspace, but also to animate private sector efforts which shall have positive reverberations on the economic health and growth in the nation.

19. "Global Cybersecurity Index 2020" International Telecommunications Union. 2021, p. 19
20. Bassem Ali Khreisan "Cyber security in Iraq: a reading in the Global Cybersecurity Index 2020." Al-Bayan Center for Planning and Studies. July 2021, p. 10
21. "Iraq sets sights on e-commerce opportunities" Conférence des Nations unies sur le commerce et le développement. July 2019

References

- Sattar J. Aboud "Cyber Crime in Iraq." International Journal of Scientific & Engineering Research. March 2014 https://www.ijser.org/paper/Cybercrime-in-Iraq.html
- Aro Omar "Law Update: Cybercrime Legislation in Iraq." Al Tamimi & Co. September 2017 https://www.tamimi.com/law-update-articles/cybercrime-legislation-iraq/
- Asmaa Khalid Jarjees Al-Tae, Hameeda Abdul-Hussain Al-Dhalimi, Adnan Kadhum Jabbar Al- Shaibani "Relationship of Cybersecurity and the National Security of the Country: Iraq Case Study." Systematic Reviews in Pharmacy. December 2020 https://www.sysrevpharm.org/articles/relationship-of-cybersecurity-and-the-national-security-of-the-country-iraq-case-study.pdf
- Bassem Ali Khreisan "Cyber security in Iraq: a reading in the Global Cybersecurity Index 2020." Al-Bayan Center for Planning and Studies. July 2021 https://www.bayancenter.org/2021/07/7266/
- "Iraq sets sights on e-commerce opportunities" Conférence des Nations unies sur le commerce et le développement. July 2019 https://unctad.org/fr/node/2223
- Farook Al-Jibouri "Iraq Cyber Security Overview." Cyber Code Technologies FZE. December 2016 https://www.linkedin.com/pulse/iraq-cyber-security-overview-announcing-our-framework-al-jibouri/
- Ali Ziad al-Ali "The Hidden Threats to Iraq's National Security." Al-Bayan Center for Planning and Studies. July 2018 https://www.bayancenter.org/en/2018/07/1549/
- "Homeland Security Did Not Fulfill the National Cybersecurity Strategy of 2017" al-Hurra Iraq. June 2021 https://www.youtube.com/watch?v=LB7u-nPnXLQ
- "Global Cybersecurity Index 2020" International Telecommunications Union. 2021 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
- National Security Advisor "Iraqi Cybersecurity Strategy 2017" International Telecommunications Union. 2017 https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/00056_06_iraqi-cybersecurity-strategy.pdf

- Mina Aldroubi "Iraq unveils plan to build and launch satellite" The National News. September 2021 https://www.thenationalnews.com/mena/iraq/2021/09/23/iraq-unveils-plan-to-build-and-launch-satellite/
- Kristen Sibbald "Iraq Parliament Suspends Draconian Cybercrimes Bill" Human Rights Watch. May 2021 https://www.hrw.org/news/2021/05/07/iraq-parliament-suspends-draconian-cybercrimes-bill