Dissecting Cyber Security:
The Balance Between National Security Interests and Human Rights

At a Glance

Over the past two decades the world has witnessed an explosion in the use of information and communication technologies (ICTs). This has become pervasive in our societies and the cyber sphere has become an essential fabric of 21st century societies. This technological revolution and evolution has opened up opportunities for the world to interact and broaden economic opportunities for many in multiple nations.

As cyberspace grows and evolves into an important part of our way of life, it has presented threats that need both international and national governance. Cyber-related crimes and attacks by hostile state actors and non-state actors has become a more serious concern of national security. We have evolved from cyber security being a matter of good organizational practices especially in the private sector, to a matter of vital national security interests as threats become more lethal and sophisticated.

This has drawn in national governments to draft a series of legislation and international treaties to mitigate such threats. The involvement of governments in cyberspace has opened both a new sphere of government power and inter-state competition, and a new arms race in the cyber realm with nations acquiring both defensive and offensive capabilities to protect against foreign powers and their own citizens. This has exacerbated existing debates on the struggles of civil liberties and government authority, with questions such as 'When do your rights begin and end? At what point do we sacrifice individual liberties for the common good, to allow the nation-state to provide for the common defense?'

The raging debates

There has been a dominant image of the desire to surrender freedoms for the objective of national security – with the right to privacy and free speech being among the most contested rights in the cyberspace. Those who are hawkish on matters of national security will propose that after the September 11, 2001, terrorist attacks there is a need to be proactive and prevent similar attacks from happening in the form of cyber-attacks; advocating for broad changes to state surveillance especially in cyberspace.

Human Rights advocates point to authoritarian regimes and their history of human rights abuses as a reason to put extensive limitations on what can be defined as a cyber-related crime. They highlight the uneven application of cyber security laws and the fact that any risks associated with cyberspace are not felt evenly, with minority groups, political and social activists, and journalists being highly targeted groups in both cyberspace and the offline security realm.

But with state and non-state actors such as hackers, terrorists and anarchists being in possession and acquiring highly sophisticated offensive cyber technologies and the growing omnipresence of the internet, there is no denying that nation-states require laws and defensive measures to ensure public safety, especially when private companies sell their offensive cyber technologies to hostile regimes. The recent scandal by Israeli software security company NSO which provided hacking capabilities to governments that penetrated the mobile devices of journalists and human rights defenders, has only amplified the calls for laws that protect human rights in cyberspace.

/ 2 ...

Human Rights organisations have warned about the deployment of mobile location tracking technologies and brute force algorithms that breach security features on devices used by governments, viewing it as an unnecessary breach of privacy.

The perceptions differ depending on the countries political systems and public views on civil liberties. However, the realist perception of cybersecurity has dominated the debate and legislative processes. Many argue that for one to enjoy the multitudes of freedoms, security must exist. Which again begs the question. 'When do your rights and mine begin?'

Walking the fine line

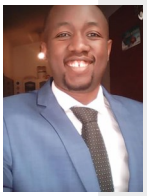
To address these divergent views, many centrists on the issue have advocated for a human rights approach to national security, specifically cybersecurity. Putting the citizen at the center and building trust between citizens and authorities can enable willing participants in the security structure of the nation. Citizens who become vigilant of cyber threats while ensuring that governments are not breaching the social contract in both cyberspace and the real world. This will require a systematic approach encompassing social, legal and security requirements of the country.

Policy-makers need to realise that the political stakes in the 21st century are too high. Multitudes of existential and internal threats adding cybersecurity concerns amongst the populous will only further discontent and mistrust between authorities and citizens and amongst citizens themselves.

This will require policy-makers to create laws that are unambiguous. An effective way in establishing a coherent and intelligent cyber law would be to enact laws that are specialized in nature to each aspect of cyberspace and the economic sector; after all, not all cybersecurity risks are the same for every individual and corporate entity in the country. This will ensure that cyber laws are not generalized, and definitions are not lost in translation.

One of the defining features among others of this century, is cyberspace. How we govern ourselves will either bring prosperity to mankind or utter destruction. The job of policy-makers is not to try and predict tomorrow by looking at yesterday's events. That is the job of academics. The job of policy-makers is to prevent the end of Tomorrow, by using their minds and imagination to stay one step ahead of the next security threat, while also not losing our humanity and inalienable rights in the process.

- TINASHE GWARIRO - 15 NOVEMBER 2021



Tinashe Gwariro

Tinashe is an international relations graduate with experience in promoting democracy, human rights and public policy analysis in Zimbabwe. He has worked as a Researcher for the International Commission of Jurists (ICJ), responsible for monitoring and documenting human rights violations arising from COVID-19 restrictions and measures undertaken by the government of Zimbabwe; initiating draft policy briefs on trends of human rights violations and possible mitigation measures; as a researcher at ICJ, part of the team that initiated the promotion of an anti-violence youth empowerment project whose goal is to promote peace through encouraging political tolerance.

Prior to that, he worked as a Program Associate with Strategic Foresight, a strategic policy advisory think-tank, where he was part of the Strategic Policy Advisory division, assisting research and writing policy briefs and security periodicals. He also conducted political risk assessment for businesses that operate in high risk African countries.

As Nhimbe's Policy Analyst Fellow, Tinashe's key responsibilities are providing research support on a broad range of policy issues related to cultural rights and artistic freedoms; and Administrative support to facilitate the work of the Nhimbe Trust Advisory Panel.