**The issue of the role of government in cybersecurity**

The UN defines the issue of cybersecurity as the state being protected against the criminal and unauthorized usage of electronic data or software, or the measures that are being taken to achieve this. Additionally, one may define the government’s role in cybersecurity as strengthening the investigation across malicious malware and cyber activity, as well as advancing cybersecurity alongside various democratic value and principles to ensure that criterial assets are met to conduct security risk assessments.

According to the UN High Commissions, the issue of the government's role revolving around cybersecurity is that it has remained a bullseye for an extensive range of cyber criminals, to which approximately 40% of 777 incidents have been undertaken by the NCSC (National Cyber Security Centre) between September 2020 and August 2021. Additionally, cybercrime costs are predicted to reach about $10.5 trillion annually by 2025 which inevitably leads to the growing concern of the misuse of information and communication technologies, which will continue to skyrocket if legal measures are not taken.

Issues of the government’s role within cybersecurity has been raised by the sole focus of identification of data preservation, protection, privacy laws and social network defenses in response to the spiteful attacks; this has been recognised by the UN through the international attempts to secure the effectiveness of the best practices, which substantially draws more attention towards raising the issue, thus foresees the transparency and oversight of the actors’ roles. While states have invested millions into the rapidly developing legislation on the issue, others may heavily lack the simplicity and basics of IT infrastructure, let alone implement policies and strategies which target the cyber-related threats that both originate from their territories.

Additionally, the UN states that the risks of government overreach can result in privacy concerns, innovation impact, trust issues as well as political misconduct. To illustrate, privacy concerns have been raised regarding the NSA surveillance programs being outwitted by the governments in the name of cybersecurity, the innovation impact could weaken the encrypted standards of building consumer’s trusts and innovation, which potentially factors into the threshold of the trust of many consumers, as a result of the public being exposed to weaknesses in the government’s own systems, undermining the universal confidence. Political misconduct has also been recognised as a requirement to share data with the government, but has been heavily criticised for facilitating state surveillance through the exploitation of personal data.

However, there is a rise in threat level in industries like healthcare which has faced over 74 ransomware attacks which jeopardies patient safety and access to secure healthcare. In addition, many small businesses cannot afford cybersecurity defenses, therefore they are deemed vulnerable to nearly 43% of cyberattacks according to the works of CISA (Cybersecurity and Infrastructure Security Agency) and NCSC, thus, the involvement of the government in this sector is viewed as vital to tackle government-mandated protocols for critical branches like enforcing laws and accountability to take down violent ransomware groups to allow governments to disrupt the criminal cyber networks.

It is inevitably crucial that we grant the acceptance of the government’s mandatory involvement in cybersecurity as we require a prime basis for the protection of cybersecurity. However, the government’s role could still in fact fuel a greater vulnerability for the security of technological platforms and could harm the public’s interest and trust towards the government’s responsibility in handling these protocols.

**Points to consider:**

* What are ways governments could tackle the advancement of cybersecurity to ensure that we meet the criteria of conducting security risk assessments?
* What legislations should governments implement to prevent the growing concern of cybersecurity misconduct?
* How can we draw more attention to the transparency of cybersecurity cases internationally?
* How can we ensure that states have governments have the basic outline of IT infrastructure to avoid delving into the overcomplexity of managing cybersecurity?
* How can we reduce the risks of governmental overreach to avoid the exploitation of personal data through cybersecurity?
* How can we ensure that all industries like healthcare and businesses can afford cybersecurity defenses?

**Some useful sources:**

<https://www.local.gov.uk/our-support/cyber-digital-and-technology/cyber-digital-and-technology-policy-team/government-cyber#:~:text=Objectives-,Context,2021%20affecting%20the%20public%20sector>.

<https://www.un.org/counterterrorism/cybersecurity>

<https://www.dcaf.ch/sites/default/files/publications/documents/CyberPaper_3.6.pdf>

<https://www.gov.uk/government/collections/cyber-security-guidance-for-business>

<https://blog.govnet.co.uk/technology/what-is-the-role-of-government-in-cybersecurity#:~:text=A%20national%20cybersecurity%20agency%20is,with%20a%20portfolio%20of%20initiatives>.