A Literature based study on Cyber Security and Climate Changes

ROSHINI SOWRIRAJAN
Senior Systems Engineer, Infosys
Email : roshvinisowrirajan@gmail.com

BADRI NARAYANAN
Founder Director, Infinite Sum Modelling LLC,Seattle, USA
Email : badri@infisum.com

Abstract: **Cybersecurity issues constitute a key concern of today's technology-based economies. Cybersecurity has become a core need for providing a sustainable and safe society. Considering the rapid increase of technological implementations, it has turned into a global necessity in the attempt to adapt security countermeasures whether direct or indirect and prevent systems from cyberthreats. With it, discourse on cyber security is increasingly prevalent on the national and international levels.The threat of hacking, or cyber influence, and control and ownership over information and intelligence is often the first imagined threat in relation to cyber security. This places the state, its infrastructure and its institutions at the centre of such threats but fails to consider the impact of cyber security on people at the individual level and their communities. Climate changes due to global warming and other factors, lead to reoccurring droughts, volatile conditions, harsh environments, exposure to unpredictable natural disasters, long winters or summer, low annual rainfall, migration and vast distances between human settlementsand other unexpected climate trends.In addition to the existing constraints and possibilities that cybersecurity and digitalisation pose for human security.This work is carried out to revisit the human-centric approaches to security in cyberspace, understanding of cybersecurity and use of cyber technologies in everyday lives of individuals and communities. It also seeks to contextualise such security influences in relation to the role of climate change and its influence on the society.**

Keywords: ***Cyber Security; Digitalisation; Human Security; Climate Change; Sustainability;***

INTRODUCTION

In the current world that is run by technology and network connections; it is crucial to know what cyber security is and to be able to use it effectively. In the last several decades; the use and spread of cyber technology; an inclusive system of information and communication technology; has rapidly increased across the globe. Cybersecurity issues constitute a key concern of today's technology-based economies. Cybersecurity has become a core need for providing a sustainable and safe society. Considering the rapid increase of technological implementations; it has turned into a global necessity in the attempt to adapt security countermeasures whether direct or indirect and prevent systems from cyberthreats. With it; discourse on cyber security is increasingly prevalent on the national and international levels.

Cyber technology and digital tools are increasingly replacing existing physical tools; and information; services and data are migrating into the digital sphere under the current trend of digitalisation. Therefore; the state of cyber security determines how digital transformation occurs. Digitalisation has changed the medium and function of everyday societal interactions and has influenced how individuals and communities relate to each other and themselves.People have begun to adopt cyber security strategies to protect their interests and securitise the cyber arena from threats leveraged by malicious actors. The threat of hacking; or cyber influence; and control and ownership over information and intelligence is often the first imagined threat in relation to cyber security. This places the world; its infrastructure and its institutions at the centre of such threats but fails to consider the impact of cyber security on people at the individual level and their communities.

Individuals' access to cyber technologies and connectivity are dependent on their locations and surrounding circumstances. The concept of human security offers an opportunity to re-centralise individuals and their communities into existing discourses in the cyber security framework. By considering cyber security from the view of human security; the analysis shifts to a focus on both the threats and the opportunities that cyber technology affords for the security of individuals and communities. In doing so; it opens discussion on how the cybersecurity framework may both exacerbate the vulnerabilities and threats posed by climate change and increase opportunities to enable resilience of individuals and communities.

Climate changes due to global warming and other factors; lead to reoccurring droughts; volatile conditions; harsh environments; exposure to unpredictable natural disasters; long winters or summer; low annual rainfall; migration and vast distances between human settlementsand other unexpected climate trends. Much of the existing infrastructure was not built considering the consequences that could arise from either climate change or cyber security; given the lack of evident need at the time it was put into place.This work is carried out to revisit the human-centric approaches to security in cyberspace; understanding of cybersecurity and use of cyber technologies in everyday lives of individuals and communities; addressing both the ways such tools enable and undermine human security. Parallelly; the rapid change in climateand increased digitalisation; seek to understand the consequent implications for human security. Considering all these; this paper analyses the existing constraints and possibilities that cyber security and digitalisation pose for human security and revisits them from a humancentric perspective of cyber securityin relation to the role of climate change and its influence on thesociety.

1.CYBERSECURITY FRAMEWORK IN CONTEXT WITH CLIMATIC CHANGES

The Framework will help an organization to better understand; manage; and reduce its cybersecurity risks. It was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders. It will assist in determining which activities are most important to assure critical operations and service delivery. In turn; that will help to prioritize investments and maximize the impact of each dollar spent on cybersecurity. By providing a common language to address cybersecurity risk management; it is especially helpful in communicating inside and outside the organization. That includes improving communications; awareness; and understanding between and among IT; planning; and operating units; as well as senior executives of organizations. Organizations also can readily use the Framework to communicate current or desired cybersecurity posture between a buyer or supplier. It is guidance. It should be customized by different sectors and individual organizations to best suit their risks; situations; and needs. Organizations will continue to have unique risks – different threats; different vulnerabilities; different risk tolerances – and how they implement the practices in the Framework to achieve positive outcomes will vary. The Framework should not be implemented as an un-customized checklist or a one-size-fits-all approach for all critical infrastructure organizations.

Analysis of cybersecurity frameworks include digital infrastructures; thereby creating a connection with cybersecurity; given that the smooth functioning of digital infrastructures is heavily dependent on the security of cyberspace. At first glance; it may seem unpersuasive to establish a link between cybersecurity and climate change. However; climate can affectdigitally operated physical infrastructures; with the high possibility of critically disrupting their systems; affecting various dimensions of human security.Environmental security concerns are therefore crucial in a region where several human security concerns intersect; such as climate change; natural resource extraction; and changes in socio-cultural and demographic dynamics as well as changes in the diverse economic interests of various actors; including local and indigenous populations

New economic activities; such as resource extraction; infrastructure development and tourism across the places; lead to changes in environments; economies and societies; all of which are increasingly integrated with the cybersecurity framework and where different interest groups emerge and interact both positively and negatively. The human and community impacts of such developments are likely to cause both immediate and long-term effects that will change existing cultures; livelihoods and relationships with the planet. In this way; human security is intimately related to climate change. However; the integration of new lifestyles and cultures driven by both demographic changes and technological advancements has brought both negative and positive incentives for the populations of the remote and rural region of the world.

The ongoing societal transformations the world faces; the functioning of society has become gradually dependent on digital infrastructures; which replace; for example; traditional physical infrastructures. Online platforms become the media through which people perform their everyday activities; their day-to-day interactions and communications; and even their livelihoods. Perhaps more importantly; public services such as education; health care and financial services are increasingly administered on online platforms. This transformation has been taking place all over the world; which offer both challenges and opportunities to its people as they digitise. These challenges do not only arise from cyber-attacks on digital infrastructure; they can also arise from climate change such as induced natural catastrophes. For example; natural disasters may disrupt communication networks and thus halt digital services; such as health care; education; everyday financing; etc. Moreover; critical infrastructures; such as energy supply; run through digital infrastructure. Disrupting these would cause drastic human suffering. The stable functioning of these systems requires resilient infrastructures.The stable functioning of digital infrastructures would promote human security; as it would enable people to access various digital services as discussed above.

2.VIEW ON TRADITIONAL CYBERSECURITY

The tendency in traditional security discourse is to view cyber security as a purely technical concept in which the integrity of a network or computer system is the referent of security. Although all the cyber threats inherently impact; the predominant object of security is still the network; system or online tool itself; while individuals and their communities are merely implied. Although this focus is still important and increasingly relevant as technology develops further; especially with emerging artificial intelligence technology and autonomous systems; there is another aspect of security that is marginalised when cyber security is presented as a predominantly technical security concept; the real-life impact of societal digitalisation for the security and well-being of individuals and communities.

The notion of "human security" was popularised within the framework of the United Nations (UN) Development Programme and based on achieving "freedom from fear" and "freedom from want". This also includes the "freedom to live in dignity." The concept promotes "people-centred; comprehensive; context-specific and prevention-oriented responses that strengthen the protection and empowerment of all people". Furthermore; the concept has been expanded to encompass not only threats to individuals and their community's survival; but also to promote security as a means of enabling individuals and their communities. In this way; human security deals both with the constraints that threat place on communities and individuals as well as opportunities for them to enable their own resilience and well-being.

3.HUMAN SECURITY ASSOCIATION WITH CYBERSECURITY

The concept of human security was developed to focus the object of security away from the state and onto individuals and their communities. In order to do so; human security proposes a bottom-up approach for understanding well-being as security centred on individuals and their communities as sites of freedom from fear; want; indignity and vulnerability. Human security re-centralises the referent object of security away from the state to individuals and their communities; and in doing so; it requires a more nuanced view of threats and opportunities for societal well-being; that transcends the concept of "threats" as viewed through a national security paradigm.

Human security relies on an understanding of security that is disaggregated by interrelated; dependent features; including health; food and communal; personal; environmental; economic and political security. These features are non-exhaustive; and the concept is adaptable to suit emerging security concerns and societal changes. At the core of human security lies human well-being through the reinforcement of human rights and development. To that degree; threats related to civil safety are also integral to the concept of human security.The continuous functioning of critical infrastructures on which individuals and communities rely for daily existence also remains relevant.

Human security addresses threats to well-being considering the increasing trend towards critical functions or work previously carried out by human being performed by machines. In this machine-dependent era; disruptions or failures of critical functions can have serious consequences for the everyday lives of humans. One emerging aspect of security that has been increasingly discussed by scholars is digital security; which focusses on the role of digitalisation in the security of individuals and communities. Digital security incorporates the foundational framework of human security as a frame of analysis in the interactions between human well-being regarding increased digitalisation. In this way; the human security is also broadly applicable to digitalisation and the evolution of cyber-based functions and their impacts on the everyday lives of individuals and communities. Human security serves as a broad framework within which the impacts of emerging trends; developments and phenomena related to the well-being of individuals and communities can be assessed; contrasting with the existing traditional security.

4.CYBERSECURITY – POSITIVE & NEGATIVE SECURITY

In understanding cyber security; technology becomes a social practice as societal knowledge and therefore re-centres the human into equations about the well-being or integrity of a cyber system.

Cyber technology in regards with discussions of human security; opportunities for enablement emerge from the ways that individuals and communities use social media and the internet generally to participate in larger society. In the same way; threats to human security regarding cyber security can be characterised as the valued aspects of social practice or knowledge that are either no longer accessible via cyber development or have become vulnerable upon their advent in cyber space.Therefore; cyber security view through the human security can be perceived as both the enabling and threatening of social practice and knowledge by cyber systems.

Telecommunication services are seen as improving the quality of life; but the current strategies do not address the potential fears or challenges local inhabitants and communities may experience through the advancement of digitalisation.Digitalisation and climate change are thus phenomena that are rapidly changing societal interactions and consequently have direct influences on the security of individuals and communities. The impacts of these phenomena on human security; are analysed both for their negative security implications (threats and constraints) and their positive security implications (opportunities and enablement). Such analysis must be guided by the underlying principles of human security; which require the identification of security elements to be made and prioritised by communities themselves.

Negative security implications at the crossover of digitalisation and climate changefrom the perspective of national security; with cyber security being conceptualised as an extension of the integrity of the technology and infrastructure in cyberspace and increasing uncertainty in the physical environment.Examples of critical infrastructures that are supported by cyber and computer-based technology include health services; finances and banking; utilities and electricity; commercial services; and industries such as aviation; energy and natural resource management. In this way; the social and economic development of various sectors of society are inherently dependent on digitalised critical infrastructure.As climate change triggers more extreme weather events and the possibility of natural disasters; physical infrastructures are increasingly vulnerable to damage. As noted above; much of the existing infrastructure was not built considering the consequences that could arise from either climate change or cyber security; given the lack of evident need at the time it was put into place.The recent cyber-attack on the US major oil and gas pipeline could become one of the most expensive attacks to an economy.This also has direct implications for communities and individuals living in the area who will bear any consequences that result from realised threats to critical infrastructure; since environmental degradation or damage may have direct impacts on physical installations or cyber systems that support critical infrastructure. Furthermore; as health systems become more digitalised and move towards e-health and tele-health services to cut costs and energy consumption; they may be vulnerable to privacy breaches as information is stored digitally; and existing critical infrastructure supporting them may be compromised. The combination of complexities; changing health interfaces themselves; the replacement of physical interfacing with digital in remote areas; potential digital divides; and the support infrastructure needed in worse climatic and geophysical conditions compounds the potential security implications for communities and individuals using and relying on such functions.As climate change drives more digital solutions to reduce energy output and physical cost; it commensurately affects data storage and accessibility. Therefore; the advent of both digitalisation and climate change has direct implications for cyber security in the view of personal security; information security; data protection and privacy for individuals and communities.

Positive conceptualisations of security implications at the crossover of digitalisation and climate change are the easiest to view with social media to enable engagement and participation across communities in the world.Social media has provided individuals and communities with the possibility to bring local issues to the global stage and to increase their participation in the development of certain activities arising from environmental or climate changerelated issues in their communities.The impact of socialnetworks on young people is significant. It is becoming increasingly clear that social networks have become part of people’s lives. Many adolescent people are using their laptops; tablet computers and smart phones to check tweets and status updates from their friends and family. Due to the advancement in technology; people are pressured to accept different lifestyles. Social networking sites can assist young people to become more socially capable. Social Media isinnovative idea with a very brilliantopportunity with additional scope for advancements. With the advancement of socialmedia many organizations are making use of this medium to better their practices. With the use of social networking; we can advertise or communicate.Such processes are expected to become part of societal development; with digitalisation providing a positive tool to assist in defining the security of individuals and communities impacted by such change. In this way; social media has enabled communities to define; actualise and advocate for the human security and well-being. Considering cyber security as an extension of security through social practice and knowledge in relation to technology; another form of positive security includes the utility of digitalisation in bringing new tools into the social practices of individuals and communities.

CONCLUSIONS

Cyber security must be understood from a human-centric perspective to assess its impacts on society. Although cyber security is predominantly viewed as impacting an invisible; intangible space; it has very real implications in the physical world. As the physical world changes as a result of climate change; these two phenomena inherently interact in impacting the security of communities and individuals. The urgency of climate change and its implications for society increase; an integrated approach to understanding the security is necessary in all aspects and need to be seriously considered from the perspective of human security and made relatable to the everyday well-being and security of individuals and communities.

ACKNOWLEDGEMENTS

Author hereby thanks Dr.S.Sridhar; Ex Vice Chancellor; the Technical Chair of this Web Conference for inclusion of my paper and the comments of Review Board while reviewing this paper for acceptance are highly appreciable and well taken to modify this final version and also Dr Badri Narayanan Gopala Krishnan; Founder Director of INFISUM; USA for his mentorship while preparing this paper .

REFERENCES

[1]. Toward a sustainable cybersecurity ecosystem https://www.mdpi.com/829490

[2]. https://arcticreview.no/index.php/arctic/article/view/1936

[3]. https://www.researchgate.net/publication/352477690_Research_Paper_on_Cyber_Security

[4]. https://www.nist.gov/cyberframework

[5]. https://www.researchgate.net/publication/323903323_A_Study_on_Positive_and_Negative_Effects_of_Social_Media_on_Society

[6]. https://www.weforum.org/agenda/2021/05/cyber-attack-on-the-us-major-oil-and-gas-pipeline-what-it-means-for-cybersecurity/

[7]. https://www.researchgate.net/publication/352477690_Research_Paper_on_Cyber_Security

[8]. https://www.mdpi.com/1311630

[9]. https://www.sciencedirect.com/science/article/pii/S1877050921014903

[10]. https://www.bitsight.com/blog/7-cybersecurity-frameworks-to-reduce-cyber-risk

[11]. https://meridian.allenpress.com/cia/article-abstract/15/2/A9/464342

[12]. https://www.researchgate.net/profile/Sina-Ayanlade/publication/362431678_Climate_Change_2022_Impacts_Adaptation_and_Vulnerability_Working_Group_II_Contribution_to_the_Sixth_Assessment_Report_of_the_Intergovernmental_Panel_on_Climate_Change/links/62ea52343c0ea87887793180/Climate-Change-2022-Impacts-Adaptation-and-Vulnerability-Working-Group-II-Contribution-to-the-Sixth-Assessment-Report-of-the-Intergovernmental-Panel-on-Climate-Change.pdf

[13]. https://wires.onlinelibrary.wiley.com/doi/abs/10.1002/wcc.565

[14]. https://www.nature.com/articles/s41558-018-0299-2?hlkid=640f283ad1524bd5af11c46baafffa79&hctky=&hdpid=37cc4487-0a8b-4708-bb43-731de4fc21bd

[15]. https://www.sciencedirect.com/science/article/pii/S2212420921001072