International Journal of Peace and Conflict Studies (IJPCS), Vol. 7, No 1, December, 2020
Available online at http://journals.rcmss.com/index.php/ijpcs; www.academix.ng
ISSN: 2346-7258 (P) ISSN: 2354-1598 (E)

Babatunde Olomu, 2020, 7(1):1-11

COVID-19 and the New Normal- Digitalization and Automation of the Global Security Sector

Babatunde Olomu, PhD

Department of Political Science and Public Administration,
Babcock University, Ilisan-Remo, Oguns State, Nigeria
E-mail: babatfund@yahoo.com

Abstract
Aside from the enormous loss of human lives, economic downturn, poverty and human insecurity effects of COVID-19 Pandemic, it has brought about indelible reality and lingering impacts in the sphere of International security sector. The paradigm shift in international security system from over seven decades of multilateral cooperation to global nationalism and its profound consequences in terms of: cybercrimes escalation; world powers rivalries; autocratic backsliding and increased authoritarianism; the crumbling of international institutions and aids for COVID-19; and weakened international cooperation system have been well acknowledged by scholars. These developments no doubt constitute the concept of the 'New Normal' in the global security space. However, the aspect of increased digitalization and automation of security operational processes across the globe represents new opportunities brought by COVID-19 Pandemic which have not received adequate attention from scholars. In fact, their reverberating consequences in the socio-economic and political spheres of both the developed and developing countries constitute matter of continuous debate in the international security discourse. Hence, this paper by adopting descriptive approach intends to identify key developments and trends in the digitalization and automation processes of global security space amid COVID-19. This will enable the researcher to explore both its areas of threats and opportunities for the advancement and sustainability of the global security sector.

Key Words: *COVID-19, the New Normal, Digitalization, Automation, Global Security Sector*

DOI URL:https://doi.org/10.36758/ijpcs/v7n1.2020/1

Introduction

Despite the fact that COVID-19 Pandemic is arguably the greatest disruption to global order since World War II (Climmino, et. al., 2020; WHO, 2020; Khan, et. al., 2020); it creates areas of strength and opportunities in the digitalization and automation processes of the global security sector. This profoundly offers alternative to the sustainability of the global world interconnectedness. Indeed, the international responses to COVID-19 pandemic offer a great blow to the over seven decades of international multilateral cooperation through stringent measures of border closure, social distancing, remote interactions, and among others. On the other hand, the vacuum created was filled by the opportunities provided through increasing digitalization and automation of global security operational processes.

Digitalization and automation have stimulated a rise in interest for technology by which processes or procedures performed with minimal human contact, especially "contactless technology" (G4s Academy Report, 2020). For instance, automation paves way for automated customer counting and flow control (to comply with social distancing rules), facial recognition, integrated fever screening and detection, remote monitoring systems, robotics and drones etc. However, digitalization or digital

transformation constitutes one of the most notable consequences of the COVID-19 crisis as the pandemic has given digitalization an immense boost. Also, through digitalization, it has been possible to stay in touch with colleagues, friends, and family. The online video conferencing apps such as Zoom, Microsoft Teams, and Google Meet have witnessed an exponential increase in new users signing up daily (Perez, 2020).

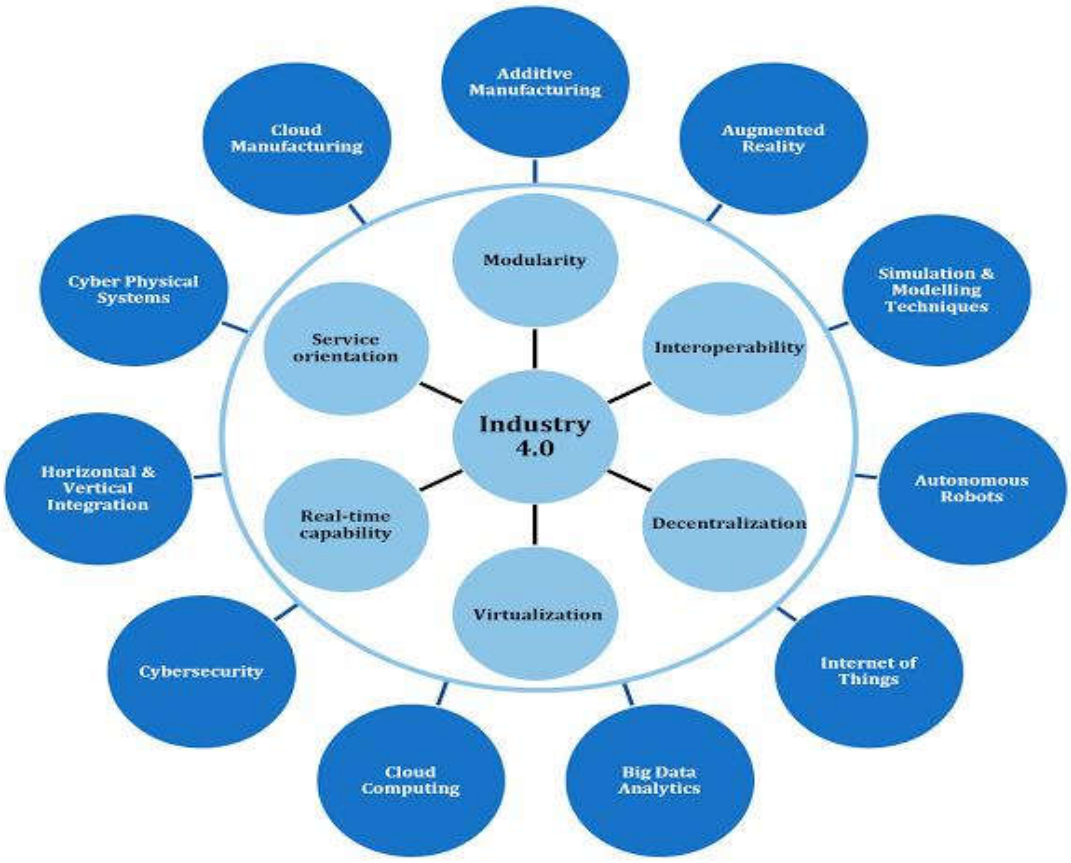
Similarly, the increasing digital opportunities of COVID-19 Pandemic in the global security sector has also increased vulnerability and risks to cyber-attacks (Humayun, et. al., 2020; Khan, et. al., 2020). For example, with the rapid growth of Zoom's popularity, Zoom is now faced with a massive backlash as security professionals, privacy advocates, lawmakers, and even the FBI warn that Zoom's default settings are not safe. As a result, many companies such as NASA, SpaceX, and countries, including Taiwan, USA, and the Australian Defence force, banned Zoom for communication (Vigliarolo, 2020). Likewise, criminals and malicious attackers have weaponised the fear and uncertainty of the pandemic to commit financial fraud and extort ransoms. Thus, the paper intends to examine the feasible areas of strengthen and newly emerging threats of COVID-19 'new normal' (digitalization and automation) in the global security sector. Its main thrust is that COVID-19 derivative opportunities via digitalization and automation can be sufficiently tapped to develop resilient cyber-security structure to combat or mitigate possible threats.

Conceptual Clarifications

Digitalization, Automation and Global Security

Digitalization implies means of empowering security sector/organisation with the skills, culture, data, and data insights draw from the technology to enable innovation and growth. It is also a way of building digital security resilience. While automation, artificial intelligence, and cloud infrastructure, among other technological advancements, present huge opportunities and create new ways for intelligence teams to communicate, pool resources, and make data-driven decisions for their organization that previously would have been either missed completely. Thus, the digital landscape of digitalization and automation makes security sector more interconnected and more exposed at any time before (*Control Risks*, 23 July 2020).

Fig 1: A Conceptual Digital Framework to Support Digital Transformation



Source: Javaid Butt. (2020). "A Conceptual Framework to Support Digital Transformation in Manufacturing Using an Integrated Business Process Management Approach". *Designs,* 4(4),17. Available at: www.mdpi.com/2411-9660/4/3/17/htm.

Key Developments and Trends in the Digitalization and Automation Processes of Global Security Space amid COVID-19

Digitalization and automation processes of global security space amid COVID-19 have brought about key developments and trends that are highly titled towards newly emerging treats and opportunities. The two sides will be sufficiently explored in this paper in order to weigh their consequences for the possibility of filling the gaps brought by COVID-19 digitalization 'new normal' in the global security sphere.

Emerging Areas of Threat of Digitalization and Automation of Global Security Space amid COVID-19

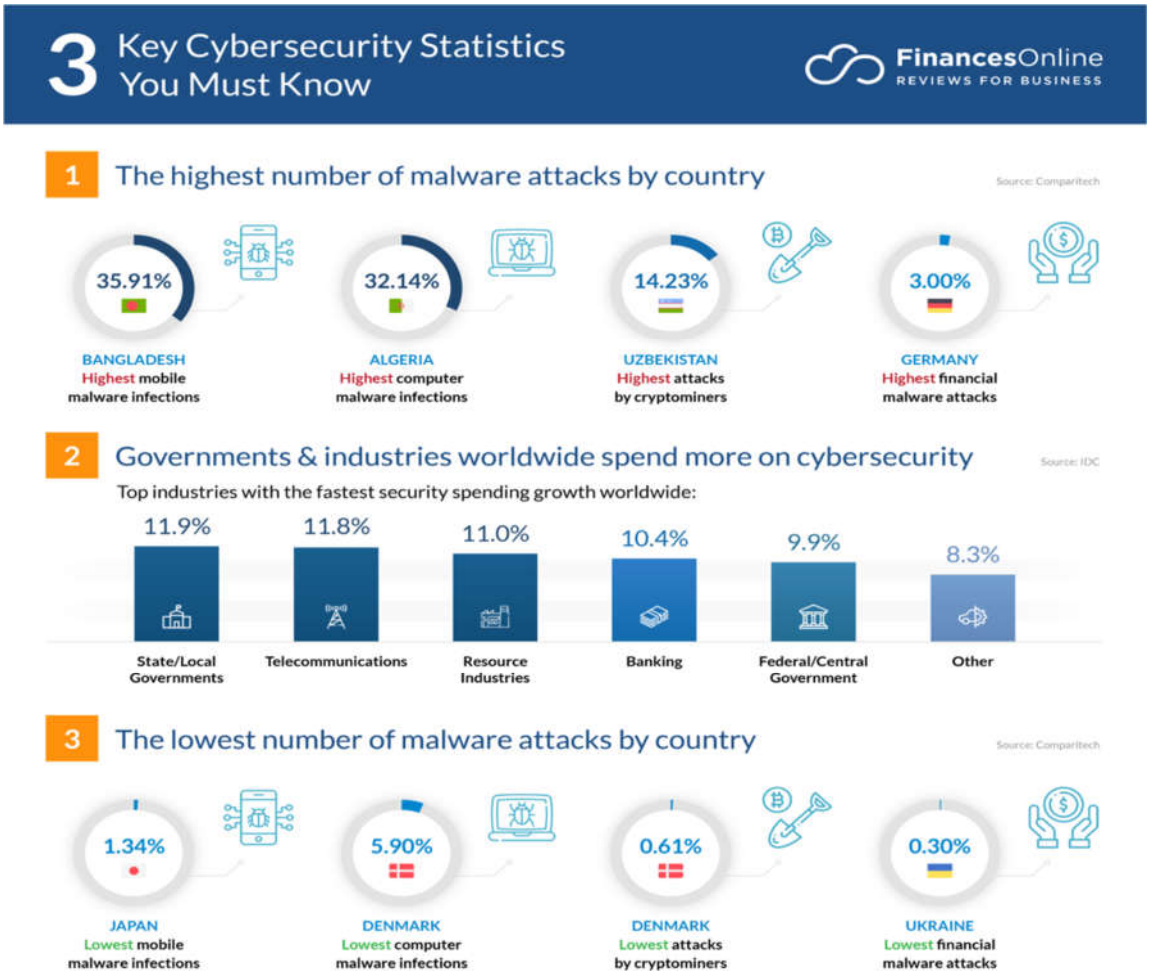
Competition between Great Powers: Evidence abounds that the increasing cyber threats amid COVID-19 goes beyond the "ordinary" criminality of fraud and theft, and even the "traditional" cyber espionage undertaken by states, but the emergence of a new era of great power competition which has raised the stakes in the cyber arena (Ford, 2020). Thus, aside from the existing problems of cyber criminality/organized crimes, there is a new layer of geopolitical threat from revisionist

states such as the People's Republic of China (PRC) and the Russian Federation; these states use cyber tools to steal technology to build up the military capabilities and prepare for devastating attacks against US and allies (Ford, 2020:1-2). The nature of this cyber threats growth can be summarized as follows:

(a) Cyber-facilitated technology transfer;
(b) Potential disruptive or destructive cyber-attacks against critical infrastructure; and
(c) Cyber-facilitated political manipulation.

The fig. 2 below further attests to increased cyber threats as a result of competition among great powers.

Fig. 2: Key/Impressive Cyber Security Statistics: 2020 Data & Market Analysis



Source: *Financeonline.* (2020). "101 Impressive Cybersecurity Statistics: 2020 Data & Market Analysis". Available at: https://www.financesonline.com/cybersecurity-statistics/

Instability due to rise in Internal Tensions: COVID-19 pave way for easy circulation of information through advanced digital technology software applications across the world, and one of the outward consequences is the escalation of internal instabilities and tensions which also constitute threats to global security. According to World Economic Forum Report (April 23, 2020), tensions are already flaring around the world, and not just in war zones. Violent protests are circulating around the world; from Brazil and India to Kosovo, Malawi and South-Africa. Police repression is also increasing from Keyan to the Philippines. Signs of fragility are not confined to poorer countries or even to marginalized communities in wealthier cities. The *yellow vests movement* has also taken to the streets of Paris, while armed protesters have marched on state assemblies in US denouncing the lock-down (World Economic Forum Report, 2020). Recently in Nigeria, ENDSARS protests is widespread across the country among the youths with support from youths in diaspora.

Cyber Threats: COVID-19 outbreak has increased vulnerability globally as hackers, attackers, and scammers take advantage of its emergencies in creating cyber threats in terms of spam messages, malware attacks etc. Besides, digitalization and automation processes of the security sector opens up new network entry points, such as cloud, social and mobile, resulting in increased and diverse risks. These new platforms stretch organization' boundaries, give rise to new threats, and require specific approaches to security (GM, 2019:8). Thus, Khan, et. al. (2020:2-4) have illustrated the top 10 cyber security threats amid COVID-19 as follows:

(1) *DDOS Attack:* This implies Denial of Services (DDos) attack. The hackers flood the organizations' websites or systems with fake or bot users to crash the normal function of the system and thus interrupt the communication channel. Of instance is a DDos attack targeted at the website of the Department of Health and Human Services (DHos) in the U.S. which flooded millions of users at a time.
(2) *Malicious Domains:* Half of the registered domains that are linked to coronavirus are malicious. These domains are used to carry out different scams, or they are used to act as a honeypot for the target users. Hackers get personal data through this procedure and then use it for their intended purposes.
(3) *Malicious Websites:* These are fake websites that operate along line with coronavirus websites. Bad actors like hackers use it to extort money from government and people by demanding for users credit and details.
(4) *Malware:* Cybercriminals are taking advantage of the current situation by spreading Malware, spywares, and Trojans through embedded interactive coronavirus maps and websites (Han, et. al., 2020). One of the main source to lure the user into clicking on the link or downloading the malware are spam emails, for which the users becomes victim through mobile device or computers (Interpol, 2020).
(5) *Ransomware:* Ransomware are launched by cybercriminals to infect the system via email attachments, links, or through working employees whose credentials are already compromised by exploiting a vulnerability in their systems (Interpol, 2020).
(6) Spam Emails: Scammers and hackers often use Spam emails to achieve their goals. This activities become worsened during COVID-19 as spam emails were being used on a large scale by intruders for extortion and fraudulent practices by pretending as legit organizations/institutions like WHO, IMF, AU and so on. Official websites of these institutions must be well-observed by clients so as not to fall a victim.
(7) *Malicious Social Media Messaging:* Hackers have dominated social media platforms like Facebook and WhatsApp. They use this medium to circulate scams and phishing tactics. They lure victims through free subscriptions such as Netflix premium free account.

(8) *Business Email Compromise:* It is activities of some intruders of Ancient Tortoise, a cybercrime organization behind several business email compromise in the past. The intruders first target the bank accounts. Then, they use the information of the customers and send them emails to change their bank information and payment methods due to the novel coronavirus. The attackers also pretend to be from legit organization or businesses (Peterson, 2020).

(9) *Mobile Threats:* This form of cyber threats are perpetuated through smartphones and gadgets which have wide usage presently. Attackers operate through an app named 'Covidlock (Ransomware)', a malicious Android app that is supposedly helping to track COVID-19 cases. The Covidlock locks victims' phones, who are given 48 hours to pay USD100 in bitcoin for recovery. The also use other android apps to perpetuate their criminal activities, for instance they could promise to offer safety kits to desperate individuals among others.

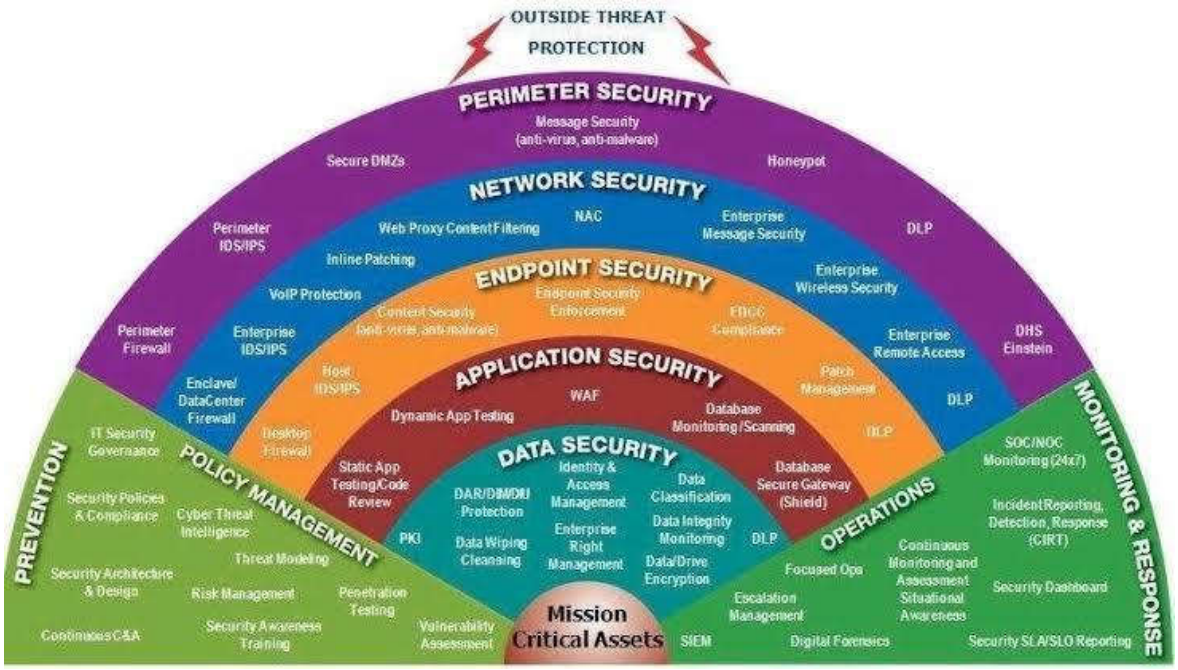
(10) *Browsing Apps:* Attackers use normal daily used browsing software to lure victims especially through propagation of fake information apps which they use to get easy access to router Domain Name System (DNS) setting in the D-Link or Linksys routers. This open the browsers automatically and display a notification or an alert from the malicious app. The alert only shows a button labelled to download a "COVID-19 Inform app". When the user clicks on the download button, it installs "Oski info stealer" malware on the device. This malware steals the browsers' cookies, stored passwords, browser history and transaction information, and many more (GoldSparrow, 2020).

Areas of Opportunities

Access to bigger volume of valuable intelligence: According to Global Security Digital Transformation Report (2019), one of the vital importance of increasing digitalization and automation of Global security processes is access to a bigger volume of valuable intelligence from embedded sensors, video surveillance, body-worn cameras and smart devices, such as tablets, glasses or watches, drives security forces to upgrade obsolete IT infrastructures. Also, with the increasing number of connected "things" estimated to reach 41 billion in the next 5 years with 5G adoption, extraction of valuable intelligence through bigger volume of digital data collection has greatly expanded (GM, 2019). Similarly, the emergence of application security, cloud security, Artificial Intelligence (AI) and digital infrastructure has massively transformed cyber security architecture.

Application Security: Digital platforms such as security websites, social media and mobile apps have become competitive landscape, and security organizations are in a hurry to deploy new application that deliver enhanced experience. Thus, through digitalization and automation processes, there is complete shifts of focus from hardware platforms to application that run on many devices. As more organizations develop applications in-house, and deploy them on private and hybrid clouds, ability to develop web applications securely will continue to be a valuable skill for risks management and security resilience through adequate evaluation and monitoring response (see Fig. 3 below). Indeed, software is the true differentiator in the age of digitalization, and many companies are using DevSecOps to secure their software in meeting the right standard. This is being achieved through alignment between security and developers, automate deployment, and making security a development standard.

Fig. 3: Cyber Security Framework Infographic



Source: Abdelhalim Mak. "Cybersecurity Framework | Cybersecurity Infographic, Cybersecurity…" Available at: https://www.pinterest.com/pin/284289795215421014/

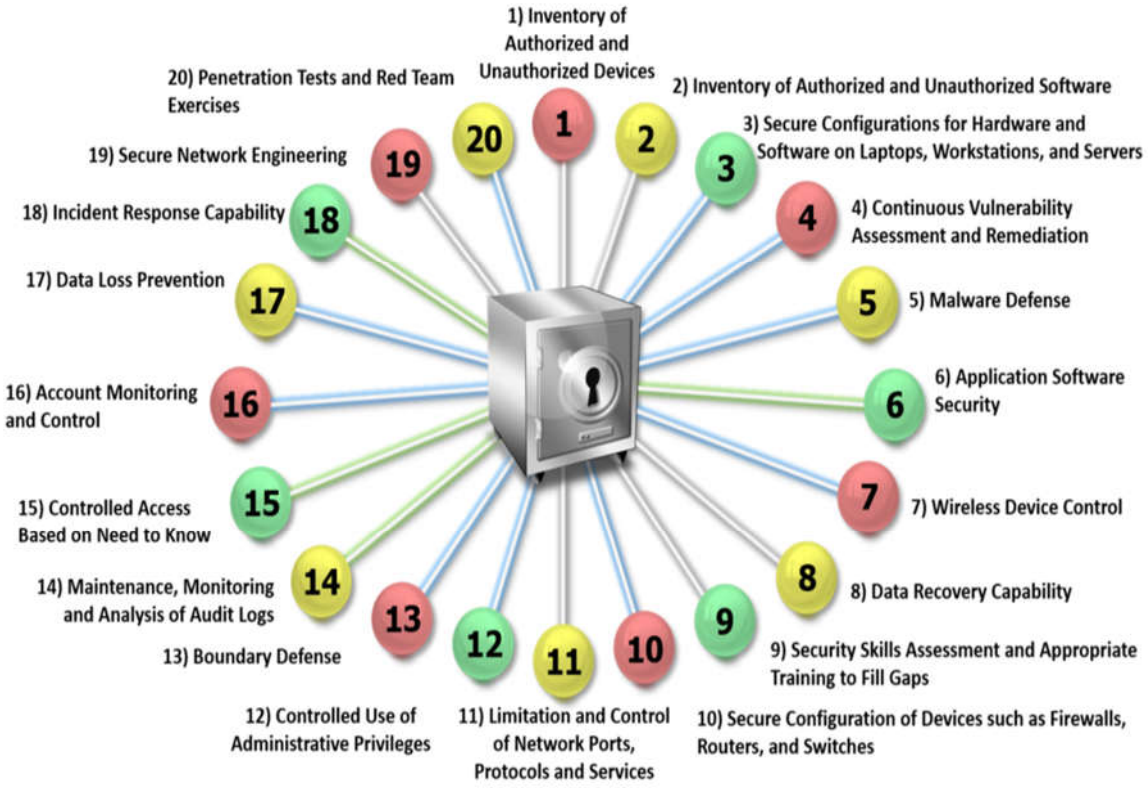
Cloud Security: Digitalization and automation has also brought about transformed experiences through cloud computing. This move involves placing critical applications and data in the cloud, despite concerns related to regulatory compliance and cyber threats. In advanced countries, regulations demand that government and semi-government organizations maintain data 'sovereignty' by hosting it locally, in their home nation. However, the region's cloud infrastructure is perceived as still emerging, with a lack of Tier III and Tier IV data (GM, 2019).

Artificial Intelligence (AI): Is also playing an important role in the digital transformation of many organizations across industries. AI powers everything from chatbots in service industries, diagnosis improvement in health care, to digital assistant support in telecommunication. Organizations are being drawn to adopt AI by the promise of benefits that include:

- Time and money savings made possible by process and task automation
- Productivity improvements and new operational efficiencies
- The ability to speed us security decisions and improve experiences based on deeper, faster insights

Digital Infrastructure Security: Digitalization and automation processes requires a robust and versatile digital infrastructure that is simple, intelligence, agile, automated, and secure (see Fig. 4 below).

Fig. 4: Cyber Security Best Practices



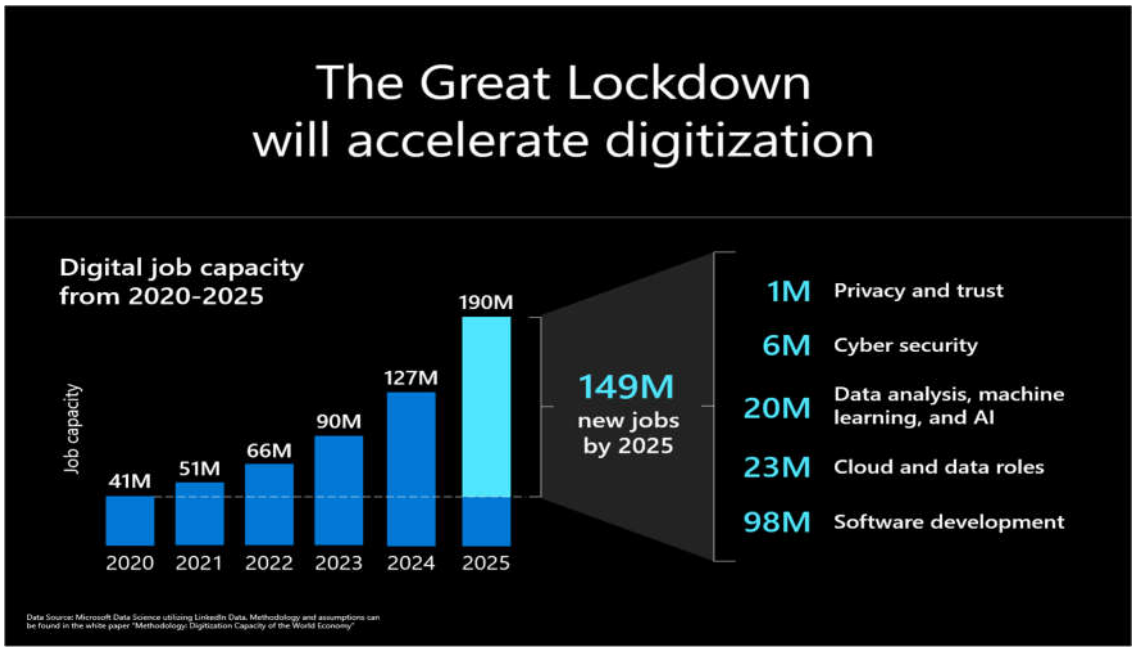
Source: *Aviationpros.* (October 21st, 2014). "Cyber Insecurity: Attacks againsts networks are increasing. Experts warn it's time for airports to boost their digital defenses". Available at: https://www.aviationpros.com/home/article/11706458/airport-cyber-security-best-practices.

Security organizations therefore need to ensure that their security infrastructure has all the resilient indicators in the fig. 4 so as to easily adapt to evolving technology and threats (relating to bigger data volume) by providing a foundation that could innovate speed to meet the changing security needs. So while traditional data centres still exist and are useful for storing and processing critical data on-premises, digital security organizations amid COVID-19 are also using a broader range of infrastructure that include cloud and edge computing sites. However, security actors must realize the fact that bigger data volume represents valuable resource which is also highly attractive to criminals in order to re-strategic and adopt more resource planning and resilience structure (as indicated in fig. 4). Thus, security forces must adopt the relevant tools to efficiently handle, securely store and analyze data to directly improve operation success, critical infrastructure resilience, identify sources of savings and adopt more adequate resources planning and risk management plans.

Growth Opportunities in the Global Security Sector: The lingering impacts of COVID-19 pandemic in terms of: Digitalization priorities through the use of remote/cloud-connected access and monitoring tools; contactless technologies such as biometrics, remote access and authentication, and multi-use analytics solutions; plug-and-play surveillance; and sensors-to-action have the possibility of generating growth opportunities in the global security sector (*SDM Newswire*, July 2, 2020). It is

on this basis Frost & Sullivan in their recent work on "Post-Pandemic Growth Opportunity in the Global Security Industry" projected that global security industry is likely to expand at a compound annual growth rate (CAGR) of 4.3 percent, garnering of $140.6 billion by 2025 from $109.3billion in 2019. The conservative forecast scenario predicts that the industry will generate $131.01 billion between 2019 and 2025, at a CAGR of 3.1 percent. In the pre-COVID-19 forecast, the industry was estimated to increase at a CAGR of 7.1 percent, generating revenue of $164.97 billion over the forecast period. Thus, though COVID-19 caused a brief slowdown in the security market, the growth potentials are highly feasible.

Fig. 5: Digital Potential Capacity



Source: Brad Smith. (June 30, 2020). "Microsoft launches initiative to help 25 million people worldwide acquire the digital skills needed in a COVID-19 economy". Available at: https://blogs.microsoft.com/blog/2020/06/03/microsoft-launches-initiative-to-help-25-million-people-worldwide-acquire-the-digital-skills-needed-in-a-covid-19-economy/

Conclusion

COVID-19 Pandemic has left remarkable impacts in the digital transformation and automation process of the global security. The opportunities created by the increasing digitalization of the global security sector considerably outweigh its likely threats particularly the possibility of great expansion and growth through well-coordinated and efficient cyber security structure. Indeed, the emerging threats as explored in this paper are not unsolvable; what is needed is the ability of the security stakeholders, actors or institutions to develop specific approaches and collectively work together in developing both cognitive and physical sense of consciousness towards curbing the dynamic nature of digital threats amid COVID-19. This will enable them to be more prepared in developing appropriate apps and programmes in countering intruding influence of scammers and hackers in the digital global security space. This study therefore intends to recommend thus:

- There is need for balanced investment in security threat detection, response and prediction capabilities. For instance, organizations should assess risks related to cloud and either mitigate or accept them, depending on their security strategy.
- Adoption of typical historical network data approach to identify a statistical baseline that represents 'normal' network behaviour, and then compare that live data against the baseline to discover 'abnormal' behaviour.
- Security organizations must identify, classify and treat their sensitive data as a valuable and irreplaceable asset. Sensitive data must be protected through discretely coded security controls to establish and maintain data quality, availability, and integrity.
- Creating a strategy, defining a policy and classifying data are the fundamental steps to starting the data security journey. These steps include defining current state and target state, classifying data, documenting data flows, creating policies and rules and forming a roadmap for the organization.
- Data Protection capabilities must evolve to support multi-cloud operations: a key feature is BYOK (bring your own key) which provides encryption with local key control.

References

African Union-UNDP. (July 2020). "The Impact COVID-19 Outbreak on Governance, Peace and Security in the Horn of Africa". *Regional Brief.*

Berman, S. P. and Gately, J. W. (2020). "COVID-19 and Its Impact on Data Privacy and Security". Available at: https://www.lexology.com/library/detail.aspx?g=dec8ccab-d74a-4bc1-9e4a-9bl5626e936.

Climmino, J. et. al. (2020). *A Global Strategy for Shaping the Post-COVID-19 World.* Washington: Atlantic Council Scowcroft Center for Strategy and Security.

Control Risks. (23 July, 2020). "Digital Transformation and Cyber Security – how to use data and technology to thrive". Available at www.controlrisks.com/our-thinking/insights/digital-transformation-and-cyber-security-how-to-use-data-and-technology-to-thrive

Council on Foreign Relations. (May 2020). International Institutions and Global Governance Program. "Challenges of Global Governance Amid the COVID-19". *Paper Series.*

Ford, C. A. (2020). "International Security in Cyberspace: New Models for Reducing Risk". *Arms Control and International Security Papers,* Vol. 1, No. 20 (October).

G4s Academy Report. (2020). "The 'New Normal' for Security Post COVID-19". Available at www.g4s.com/news-and-insights/2020/06/03the-new-normal-for-security-post-covid-19

GBM. (2019). "The Unspoken Truth: The Role of Cybersecurity in Breaking the Digital Transformation Deadlock". GBM 8th Annual Security Survey.

GoldSparrow. (2020). "Oski Stealer". Available at: https://www.enigmasoftware.com/oskistealer-removal/.

Han, J. W., Hoe, O. J., Wing, J. S. and Brohi, S. N. (2017). "A Conceptual Security Approach with Awareness Strategy and Implementation Policy to Eliminate Ransomware". *Proceedings of the 2017 International Conference on Computer Science and Artificial Intelligence*: 222-226.

Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M. and Mahmood, S. (2020). "Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study". *Arab. J. Sci. Eng.:* 1-19.

Interpol. (2020). "COVID-19 Cyber threats". Available at: https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats.

Khan, N. A., Brohi, S. N. and Zaman, Noor. (2020). "Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic". *ResearchGate.* Available at https://www.researchgate.net/publication/341324576.

Perez, S. (2020). "Videoconferencing apps saw a record 62M downloads during one week in March". Available at: https://techcrunch.com/2020/03/30/video-conferencing-apps-saw-a-record-62m-downloads-during-one-week-in-march/.

Peterson, P. (2020). "Business Email Compromise (BEC): Coronavirus a Costly New Strain of Email Attack". Available at: https://www.agari.com/email-security-blog/business-email-compromise-bec-coronavirus-covid-19/.

SDM Newswire. (2 July, 2020). "Security Industry Expected to Fare Well Post-COVID-19". Available at www.sdmmag.com/articles/98257-security-industry-expected-to-fare-well-post-covid-19

Vigliarolo, B. (2020). "Who has banned Zoom? Google, NASA, and more". Available at: https://www.techrepublic.com/article/who-has-banned-zoom-google-nasa-and-more/.

World Economic Forum Report. (23 April, 2020). "We Urgently need major cooperation on global security in the COVID-19 era". www.weforum.org/agenda/2020/04/we-need-major-cooperation-on-global-security-in-the-covid-19-era/