CONASENSE 2021 SYMPOSIUM

Building an Agile Co-Innovation Framework for Addressing Emerging Technological Challenges

Prof.dr Milica Pejanović-Djurišić

Faculty of Electrical Engineering, University of Montenegro

New Reality

Geo-politics → Geo-technology

Countries' positioning in regard to complex technology environment could be considered today as a substitute to geopolitics in the the nineteenth and twentieth centuries as new technologies (artificial intelligence (AI), big data (the cloud), robotics, biotech, advanced manufacturing, the Internet of Things (IoT), 5/6G, nano-engineering and -manufacturing, quantum …) will do much more than just transform science and research, already demonstrating far-reaching social, economic, and geostrategic consequences.

New technologies will determine how we all live and function and it is clear that the race for technological leadership among the world's powers—will be an important part of the global order transformation. Those countries that can create and implement cutting-edge technologies—while being able to adapt to those technologies at the same time—will realize enormous economic and geostrategic benefits in the decades to come.

Current Environment

In such circumstances, countries around the world increasingly recognize that they must lead in tech based innovation if they are to be prosperous and secure today and in the future. In our societies activities of political, economic, social and cultural life already depend to a large degree on digital connectivity

The core of the current development and security environments is information and communications continue to be the key to any advancements and progress. An example of unprecedented change governments across the world are going through is a move towards a network centric approach to their communications, including operations in conflict zones to homeland security and disaster recovery operations. NCW is becoming an emerging response to the information age. It focuses on NCW potentials related to effectively linking or networking various segments of society.

Keeping with the changed environment

The rapid technological change, which comes with disruptive innovations, has obviously changed the character of security threats, including conflicts and warfare.

Today's most pressing cyber threats directly target principles of freedom and democratic values, as a means of undermining entire civilizations—first as a precondition for political change, and possibly in lieu of military conflict altogether.

There is an open question if governments' strategies and concepts have been appropriately amended to keep up with this change. Moreover, as historically, the government sector hasn't been perceived as the one embracing fast and/or disruptive changes.

As the technology superiority is becoming more and more of an issue, there is no alternative to understanding the challenges inherent to innovating for the contemporary security environment and act accordingly.

New Risks

- Next generation technology solutions, digital platforms and applications have created a number of new, low cost, dynamic possibilities.
- However, a Pandora's Box of next generation risks has been opened. Following the fact that the digital world is characterized with connectivity and open architecture, keeping up with security and risk management solutions is a must.
- These risks have to prioritized following specific operation in every particular case. Then, they have to be managed using smart tools to quickly detect threats and attacks and respond in real time.
- Ensuring security of data and assets is of paramount importance at every level of operation, for enabling innovation and overall economical and social progress. Choosing the right approach will create environment for keeping the pace with the speed, safety, and growth required in today's digital economy.

Cyberspace as a new domain

Facing the rapid pace of technological advancements, further stressed in these times marked with pandemic, authorities, as well as individuals, are showing readiness to embrace new opportunities offered by ICTs.

At the same time, as a direct consequence of vulnerabilities of new technologies, rapid evolution of various cyber threats due to malicious use of ICTs by all kinds of actors present in cyberspace is becoming a new norm.

As cyberspace is the technical foundation on which the world is increasingly relying, cyber readiness and resilience are critical for ensuring positive trends in adopting emerging technology solutions.

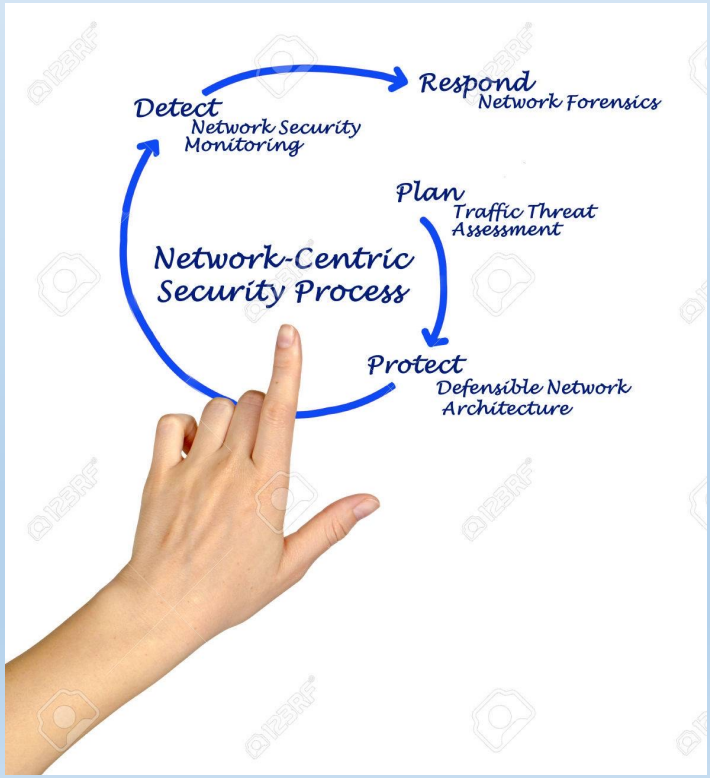
...Challenges...

- A myriad of threat actors, many stakeholders (civilian authorities, military, industry, civil society organisations, individuals etc.), the rapid technological change that expands the cyberattack surface (increasing vulnerabilities).
- Burden sharing in emerging multi polar world of old and new adversaries.
- A cybersecurity gap as adversarial cyberattacks are still outrunning defender security improvements in technology, processes and education.

Technology Responses

It’s obvious that the challenges are particularly acute in the area of communications, which are typically characterized by user mobility and unpredictable transmission channels. In parallel with demanding security requirements and the need for interoperability among disparate systems, including legacy systems, these characteristics make it difficult to meet the needs and expectations of specially vulnerable applications.

Several new system and network design paradigms have emerged including software-defined radio and networks, and named data networking; along with progress in network security, routing, dynamic resource allocation, and media access control. These developments are playing important role to improve the feasibility of truly network centric operations as the next generation of platforms needs to leverage more modern communication technologies.



Embracing fully these developments conditions will be created for the next step in managing the security of communication networks: migration towards application-based networks, where the required level of security would be maintained.

Building Effective Partnerships

- In order to be able to develop and implement solutions based on new technologies, while providing the necessary level of security, governments have to become more open for partnerships with other actors of the innovation ecosystem and more encouraging for ideas in its own ranks, while accepting discovery-driven planning and some elements of the lean-startup methodology.
- In doing so, it is important to emphasize the importance of understanding the challenges inherent to innovating for the contemporary security environment and a level of uncertainty of a future threats. And that ambiguity might be what actually has led to hesitation when it comes to adding stronger innovative aspects into course of action.
- However, changes in international security environment we are witnessing in the last years have brought a higher level of certainty when it comes to the nature of threats , creating an environment where modernization is a must… and the other name for modernization nowadays is innovation which will enable rapidly adaptable solutions based upon timely reassessments of the changing security environment.

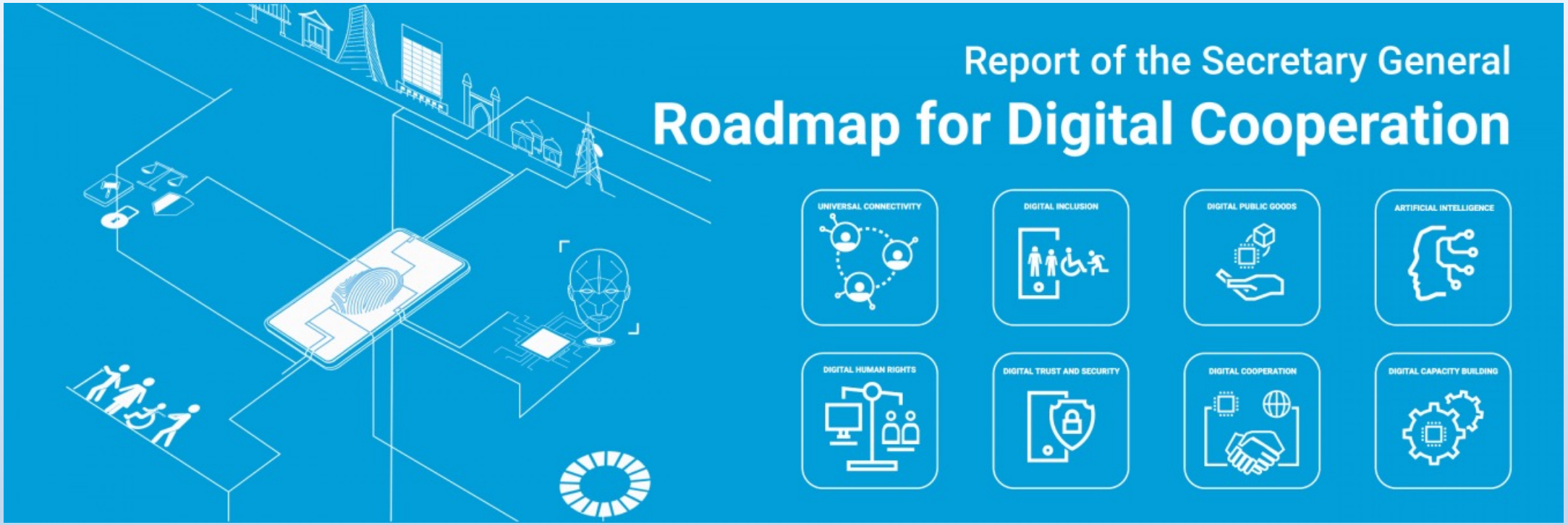
Way forward

- Call for a change—architecturally and organizationally
- Increase of government funding and other resources across the following activities: defending own networks, ensuring mission-critical networks and cyber aspects of mission assurance, providing high-quality cyberspace situational awareness, designing policies and practical tools to integrate sovereign cyber effects designing responses to the grey zone cyberattacks, and enhancing cooperation with like-minded regional and global partners.

MOVING STRONGER TOWARDS INNOVATING AND BUILDING NEW CAPABILITIES AND CAPACITIES

in coordinated partnerships with diverse stakeholders: governments (local and national), academia, entrepreneurs, venture capitalists, incubators and accelerators.

First Steps



https://www.un.org/en/content/digital-cooperation-roadmap/

The challenges of the 21st Century require common understanding, a shared vision of the future, and most importantly, joint action. This is the context in which the UN Secretary-General launched Roadmap for Digital Cooperation in June 2019, following an extensive process of multi-stakeholder consultations that began with the Secretary-General's High-Level Panel on Digital Cooperation.

UN Roadmap

High-level Panel on Digital Cooperation strongly emphasizes the need to strengthen cooperation in the digital space. Not only the critical importance of cooperation to create “digital public goods” is underscored, but also that digital technology needs to become a seamless part of service delivery for governments and development practitioners.

Emphasizing the importance of multi-stakeholder approaches, the Roadmap calls for concrete action in eight areas:

- Achieving universal connectivity
- Recognizing and promoting digital public goods
- Including the most vulnerable in the digital ecosystem
- Building digital capacity across all countries
- Ensuring the protection of human rights in the digital era
- Supporting global cooperation on Artificial Intelligence
- Promoting digital trust and security to advance the SDGs
- Building a more effective architecture for digital cooperation

UN – Cybersecurity initiatives

1. Group of Governmental Experts have focused on the following topics:

- Existing and emerging threats
- How international law applies in the use of ICTs
- Norms, rules and principles of responsible behavior of States
- Confidence-building measures
- Capacity building

2. Through resolution 73/27, the General Assembly established an **Open-Ended Working Group (OEWG)**, in which all UN Member States were invited to participate. The Group convened for the first time in 2019 and report back to the General Assembly in 2020. It concluded its work with the Final Report in March 2021.

The OEWG process provided the possibility of holding intersessional consultative meetings with industry, non-governmental organizations and academia.

Partnerships for Innovating

Diverse partnerships and other changes will require governments to be more significantly involved themselves in the provision of cybersecurity.

At the same time, only the coordinated wide innovation system will be able to provide necessary change of the technical architecture and underpinnings for defending against cyberattacks, so that networks would be defended, mission-critical networks ensured, high-quality cyberspace situational awareness provided, policies designed and practical tools created, in the situation when existing trusted platforms have been found to have backdoor access and mobility continually challenges the definition of securing to “the edge”.

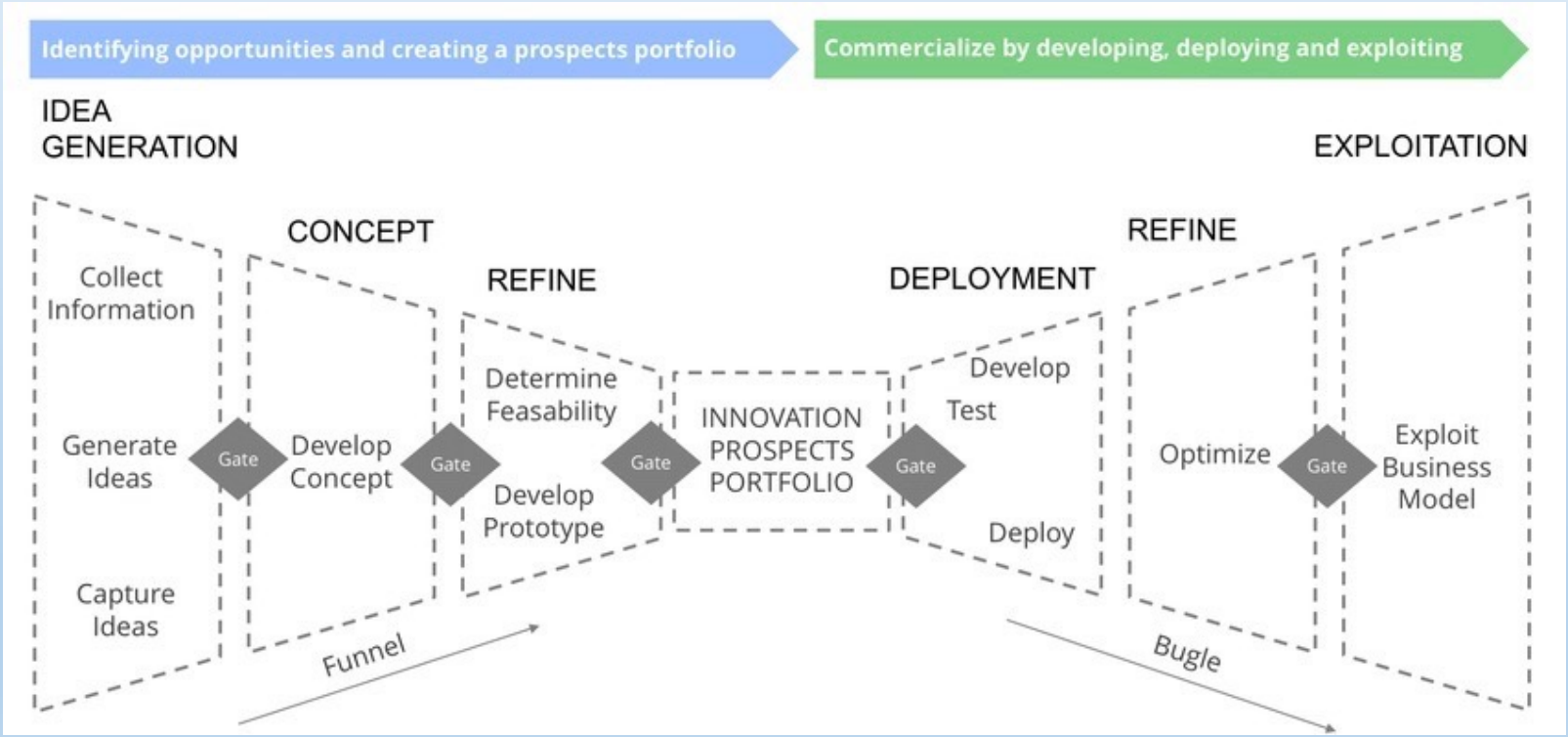
Agile Innovation

- In order to be effective, partnerships have to be characterized with the right technology vision for the future. At the same time, they should be in a position to offer their past technology experience, blueprints, and accelerators to ensure the success. This kind of know-how accelerates and de-risks initiatives, leading to a fast, secure and successful digital transformation.
- This will be further ensured through combining a high-performance culture, knowledge and expertise from academia.
- Agile innovation, i.e. the creation of differentiated digital experiences, includes: a high-performance stakeholders, Agile process, and creative mindset. In such framework, fast development and a high quality output depends on:
  - Shared success
  - Agile methods
  - Knowledge transfer
  - Co-creation

Structured Framework

A well defined and implemented innovation process provides the basic framework for establishing the necessary environment for agile co-innovation.

The Agile Co- Innovation Framework is a system for the structured development of innovations through full cooperation of coordinated diverse partners. Such Framework , in addition to agile methods, also has a clear structure for roles, artifacts and its main strength is the integrated roadmap for reaching the required level of technology maturity, while minimizing cyber risk.



Source: F.Schultheiss “The Agile Innovation Framework: A Next Generation Innovation Model”

The structured co-innovation framework is the key for effective governance of cyberspace which is *per se* technologically extremely demanding operational domain as there are numerous internal and external partners involved as well as numerous platforms, frameworks, and designs.

That is why NCW, in the situation when many processes are deployed globally, with geographic management and risk mitigation being a challenge, is an option of choice. Such structure usually outperforms other mechanisms, enabling better performance of joint efforts in a complex environment characterized with diverse actors, having the same goal:

MASSIVE, PERSONALIZED, FAST, RELIABLE, SAFE… DIGITAL SERVICES AND APPLICATIONS

Conasense

Thank you!

Q & A