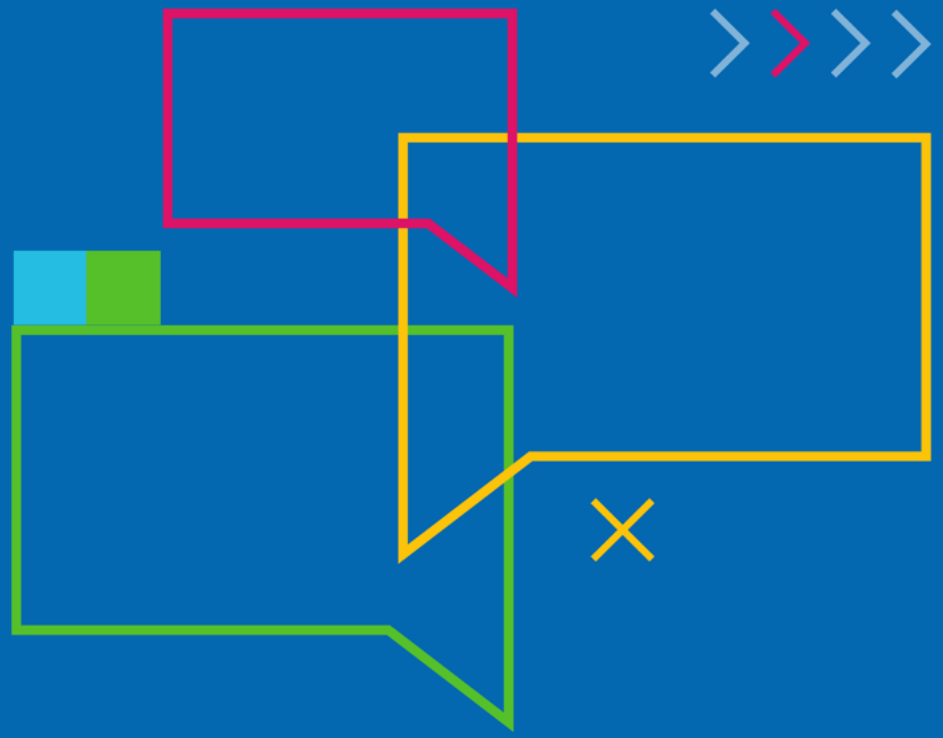


THE DIGITAL HOUR

UNDP Digital Hour on Cybersecurity: How can we enhance Cyber Resilience for our partner countries?

July 2021

Agenda

- Cybersecurity challenges
- Cyberspace protection layers
- Cybersecurity ecosystem
- Skills needed
- UNDP’s programming approach to cybersecurity
- Bosnia and Herzegovina case

Today's speakers from UNDP in Bosnia and Herzegovina

Kemal Bajramović
Head of Experimentation at Accelerator Lab
kemal.bajramovic@undp.org

Marina Dimova
Innovation and Integration Cell Lead
marina.dimova@undp.org

Edin Serezlić
Human Rights and Security Sector Lead
edin.serezlic@undp.org

(in order of appearance)

UNDP Digital Hour on Cybersecurity: How can we enhance Cyber Resilience for our partner countries?

Country cybersecurity ecosystem explained

Kemal Bajramovic, UNDP Bosnia and Herzegovina

July 2021

Cyberspace security challenges

- **Abusive content** — Spamming, harmful speech, child abuse, violence...
- **Malicious code** — Unwanted files/ programs intentionally stored on a computer system to cause damage.
- **Information gathering** — Collecting information about a potential target for future attack and exploits
- **Intrusions** — A successful compromise of a computer system or digital service
- **Denial of Service** — Overload or shutdown of service preventing its use.
- **Informatio n content** — Unauthorized access/ modification of information
- **Frauds** — Masquerading, copyright infringements...

Other — All incidents which do not fit in one of the previous categories

Incident Taxonomy according to eCSIRT.net

UNDP DIGITAL

Vulnerabilities to be exploited?

UNDP DIGITAL

vijeceministara.gov.ba **eizbori.izbori.ba** **bhrt.ba** **sia.ba** **vladars.net** **fmup.gov.ba** **mojtelemach.ba** **olx.ba** **ephzhb.ba** **centrotrans.com**

Plaintext HTTP server doesn't redirect to HTTPS	This plaintext HTTP server doesn't redirect to HTTPS, leaving its user vulnerable to content sniffing and active network attacks. From late July 2018, Chrome marks plaintext web sites as 'not secure'. We recommend that a redirection is added as soon as possible.
No support for STARTTLS	One or more servers lack support for STARTTLS, which means that they do not support email encryption at all.
HTTPS server redirects to plaintext HTTP	This HTTPS server redirects to plaintext HTTP, defeating encryption and exposing its users to content sniffing and active network attacks.
Invalid external destination	This policy uses an external report destination that is not authorized because the permission record doesn't exist. Please refer to RFC 7489, Section 7.1, for instructions how to correct this problem.
Certificate doesn't match hostname	The provided certificate doesn't match the expected hostname. (expired 6 years 5 months ago)
Nameserver provides a recursive service	Authoritative servers must not provide recursive services. This is necessary to minimize the chances of an attacker poisoning the nameserver's cache by sending queries that resolve to bogus information.
Redirection from HTTP to HTTPS not to the same host	When HSTS is used, the plaintext port should redirect to the HTTPS variant of the same hostname. This approach ensures that HSTS is enabled on that hostname, even if later the client is sent elsewhere. A redirection to another host is only safe if it is for a parent host that has HSTS with includeSubDomains enabled, but that's not the case here.
XSS auditor blocking is dangerous	Your configuration requests blocking when XSS attacks are detected, which is potentially dangerous as it allows attackers to selectively disable portions of JavaScript code. The only safe approach is to explicitly disable browser-based XSS protection.
Cookie is not secure	This cookie, which has been sent over an encrypted channel, doesn't have the secure flag set. As a result, an active network attacker can easily recover it.

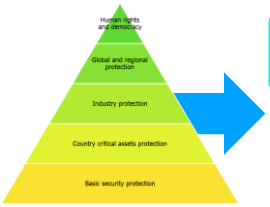
Cyberspace protection levels | Cybersecurity work areas

Human rights and democracy protection	• Core values, cyber ethics and democracy
Global and regional protection	• Cyber norms, cyber diplomacy, cyber defense
Industry protection	• Support businesses and industry protection against cyber crime, espionage
Country critical assets protection	• Essential and important public and private services
Basic security protection	• Cyber hygiene • Citizens‘ safety

National cybersecurity system

by ENISA overview of cybersecurity

National Cybersecurity ecosystem



LEVEL OF ENGAGEMENT **STRATEGIC**

Cybersecurity Strategy

Envisions the system to ensure a high level of Cybersecurity

- Defining the strategic objectives, concrete policy actions, and a governance framework to achieve the goals and priorities;
- identifying measures related to preparedness, response, and recovery, including cooperation between the public and private sectors;
- indicating education, awareness-raising, and training programs;
- identifying various actors involved in the implementation of the Strategy...

Law on Cybersecurity

Defines procedures and measures to achieve a high common level of information security

- Defining the role and powers of competent authorities;
- supervision of government organizations, operators of key services, and providers of digital services in the implementation of the Law, including misdemeanor provisions;
- defining operators of key services and providers of digital services;
- defining bodies responsible for incident prevention and protection (CSIRTs)...

National or Sectoral Cybersecurity Competent Authorities

Regulate and monitor the implementation of the Law at the national level and sectoral level

- Liaison function to ensure cross-border cooperation;
- cooperate with the relevant law enforcement and data protection authorities...

Computer Security Incidents Response Team(s) – CSIRTs

First responder to cyber security incidents by identifying, reviewing, coordinating incident resolution, documenting, and reporting findings

- Reporting incidents to the in-country CSIRT network and law enforcement agencies;
- Maintaining awareness of, and implementing procedures for, an effective response to computer security incidents;
- Staying current on functional and security operations for the technologies within their area of responsibility...

UNDP DIGITAL

- Academia & Research
- Civil Society Organizations
- IT Vendors
- Internet Service Providers
- Law enforcement agencies
- System administrators and others

OPERATIONAL

- Financial infrastructure
- Health
- Energy
- Banking
- Transport
- Water
- Digital infrustructure
- Digital service providers
- Public administration
- Postal and courier services
- Other

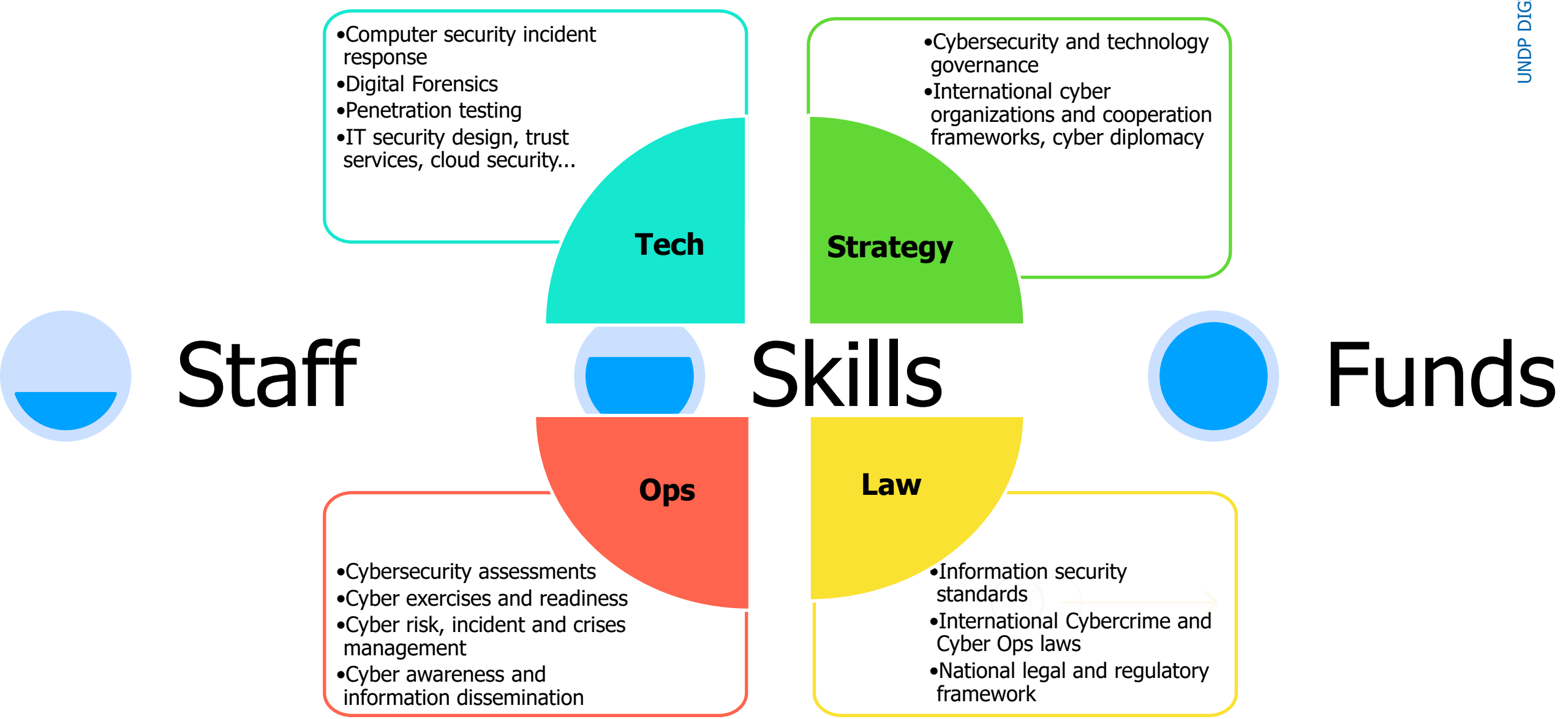
Implement cybersecurity requirements and report cybersecurity incidents

- Businesses
- Citizens

Empower & protect

FIELDS OF ENGAGEMENT

Skills needed



UNDP Digital Hour on Cybersecurity: How can we enhance Cyber Resilience for our partner countries?

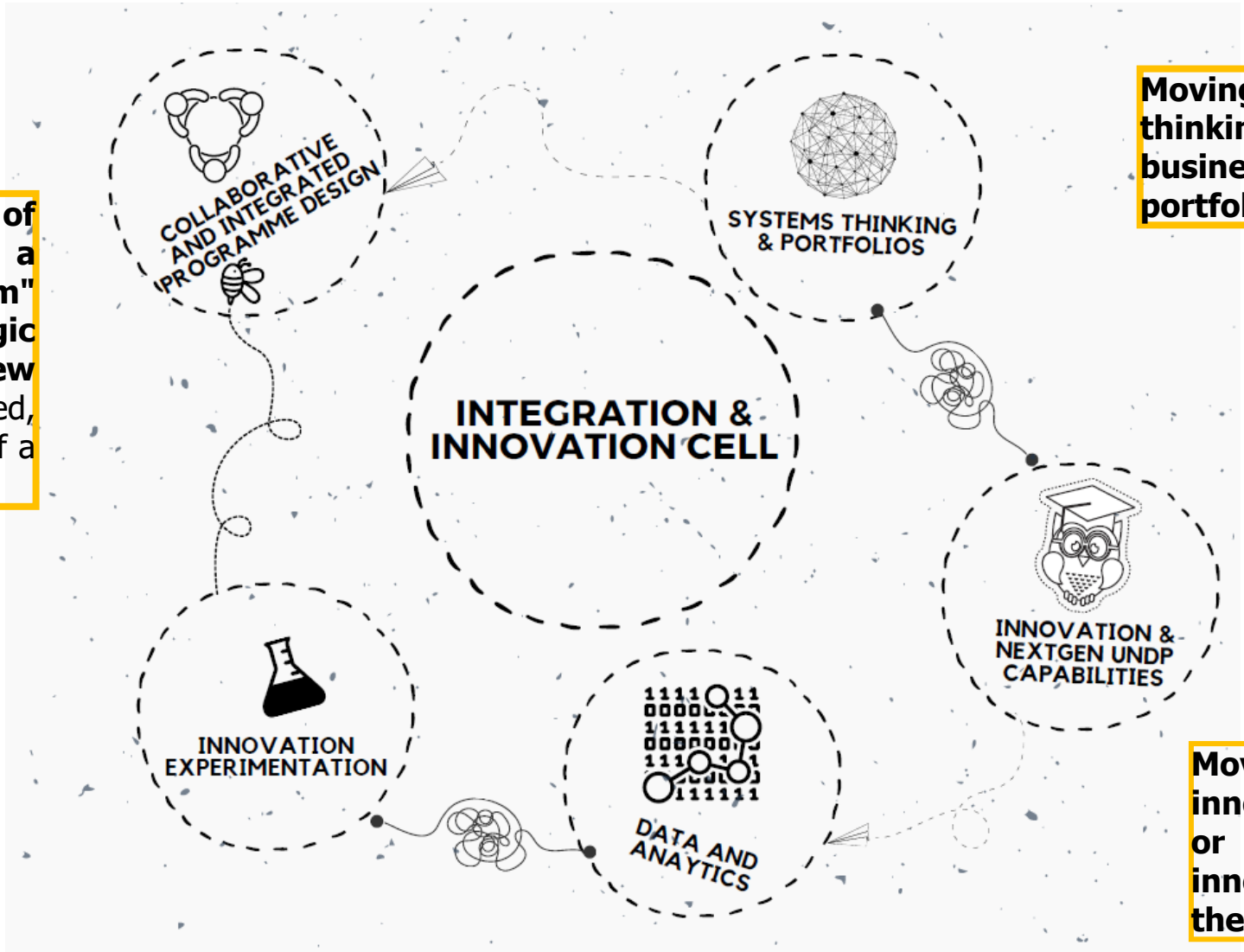
UNDP' programming approach to cybersecurity

Marina Dimova, UNDP Bosnia and Herzegovina

July 2021

UNDP Bosnia and Herzegovina programming approach to cybersecurity

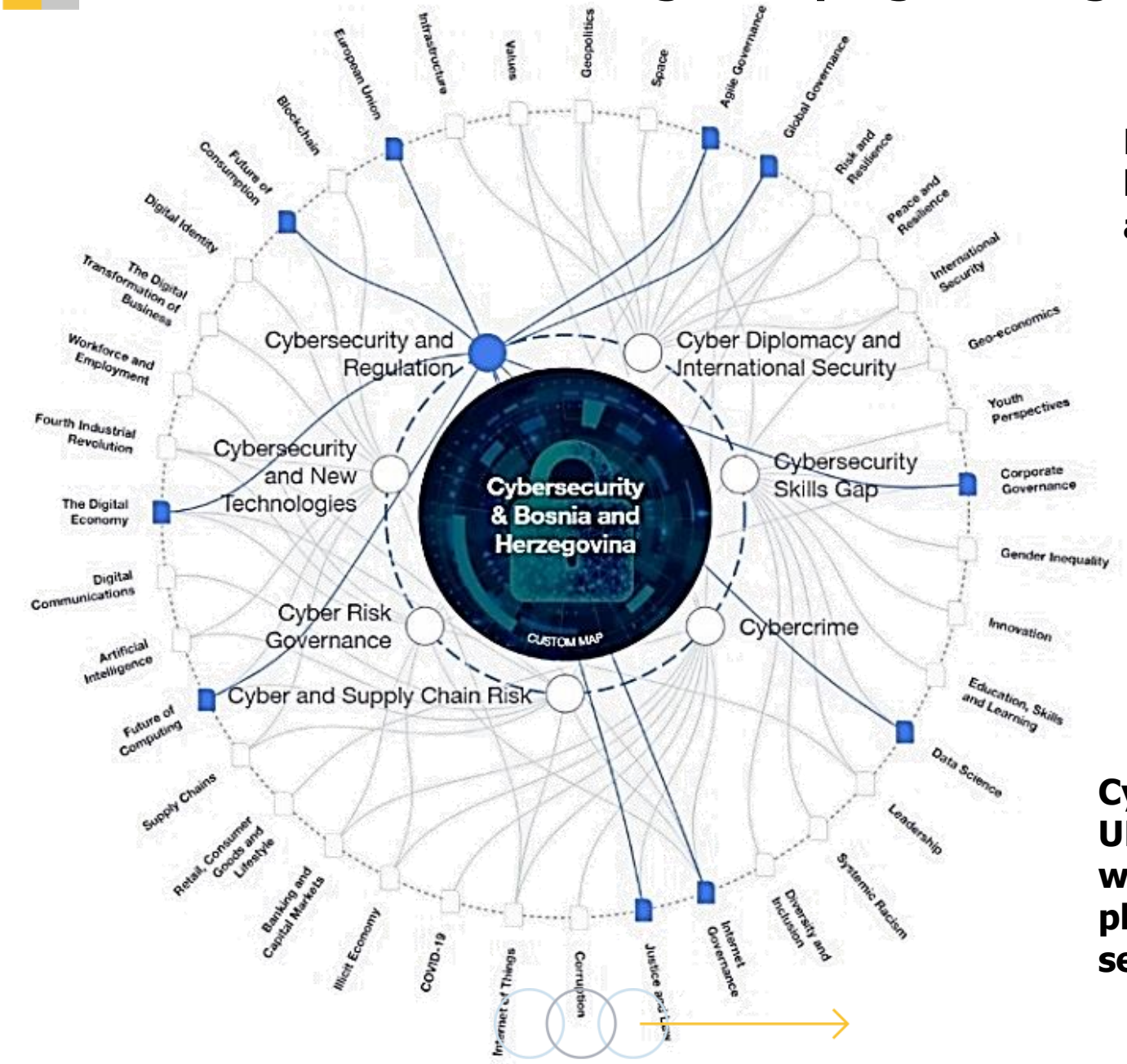
Moving from the habit of "new project design by a consultant or a small team" to a collaborative strategic conceptualization of new interventions (integrated, system-thinking and as part of a wider portfolio)



Moving from sector-based thinking and "doing business" to a network of portfolios

Moving from a stand-alone innovation acceleration unit or lab to an embedded innovation function within the UNDP team.

UNDP Bosnia and Herzegovina programming approach to cybersecurity



Entering the cybersecurity system-building in the country from a complex and holistic perspective.

Complexity analysis to identify the strategic entry point for UNDP's engagement in cybersecurity.

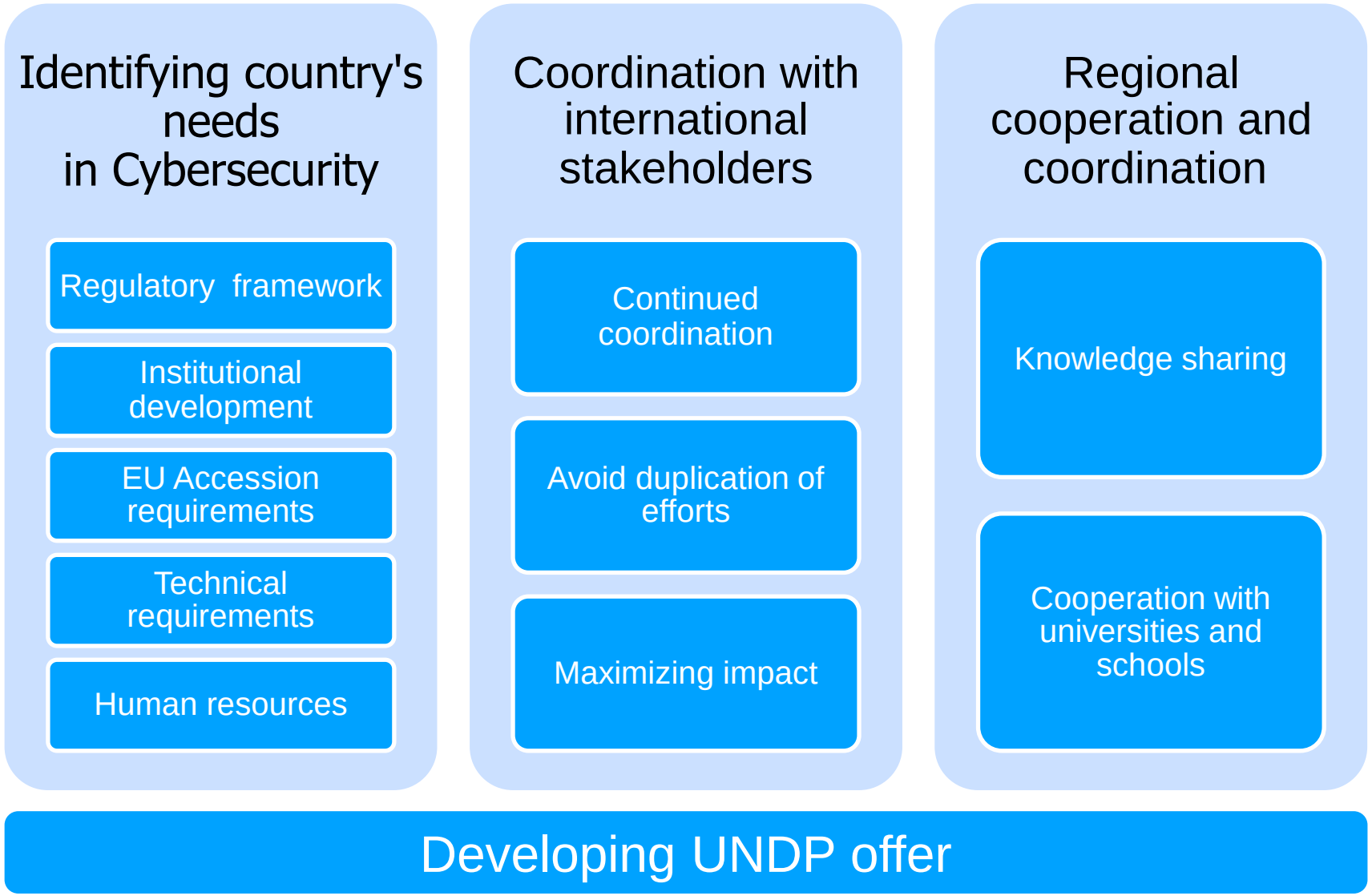
Cybersecurity conceptual framework: UNDP strategic offer and direction, which serves as an "investment platform" and cuts across different sectors

UNDP Digital Hour on Cybersecurity: How can we enhance Cyber Resilience for our partner countries?
Cybersecurity in Bosnia and Herzegovina

Edin Serezlic, UNDP Bosnia and Herzegovina

July 2021

Cybersecurity in Bosnia and Herzegovina



UNDP
DIGITAL

Q&A

Please use chat for your questions

Thank you!