The Cybersecurity and Privacy Protection in the 28 Northeast-European Countries Consulting Program

Preliminary communication materials

June 2021

目录

页码

A. Preliminary Working Plan

We will present a detailed plan for the content of each sub-work based on the current project requirements

Working Content of the Overall Project

Original requirement contents

1 Tracking and interpreting cybersecurity legislation and bills

- Sorting out national strategies, policies, laws, and regulations in cybersecurity in various countries
- Interpret the cybersecurity strategies, key laws, and regulations of selected nations
- Monthly Report

2 Have the insight of the trends of cybersecurity situation in various countries

- Sort out the documents of cybersecurity regulatory organizations and industry organizations in various countries
- Interpretation of the cybersecurity reports and related documents from selected regulators, key industry organizations, and analysis of ICT industry security ecological trends
- Monthly Report

3 Having the insight into the maps of the Cybersecurity Stakeholder

- Sort out information on organizations and key stakeholders of cybersecurity regulators, industry associations, customers and export the stakeholder maps
- Regularly updated key stakeholder maps

4 Recognize and participate in summits and send out the conference conclusion

- Identify cybersecurity conferences or summits or events, attend and summarize the conclusions and make recommendations based on the conferences

5 Support the writing of the conference material of the Cybersecurity Summit events

- Support the material writing and operation of the summits, forums, associations, and other events about cybersecurity

Reference Source: Roland Berger

Detailed Working Content of the Cybersecurity Legislation and Bills

Mission 1: Tracking and Interpreting Cybersecurity Legislation and Bills

Key problems to be researched in the project

Overall National Cybersecurity Strategy

> What is the overall positioning of national cybersecurity strategies? (level of importance, geopolitical bias)
> Specifically, in which industry sectors are more focused on the regulation of cybersecurity?

Policies and Laws

> What are the relevant regulatory authorities? What kind of policies, laws, and regulations has been issued?
> In comparison, which countries have more regulatory requirements? What are the differences in regulatory requirements between various countries?

Case Studies and Interpretation of Laws and Regulations

> What kind of policies, laws, and regulations focuses on the key countries? What are the specific requirements? What past jurisprudence do we have?
> What kind of enlightenment for the Compliance of Huawei they can get from the policies, laws, regulation, and jurisprudence?

Related Regulation and Laws

> What are the international, national, and industry standards that match the relevant policies, laws, regulations?

Methodology and Resources

> Roland Berger's past project experience
> External Expert Interviews
> Desk Research
> Professional Database of laws and regulations
> Official public Information of government and regulatory agencies

Working Purpose and Output Content

> The purpose is to form an understanding of the strategic positioning of cybersecurity in each country, generate a panorama of cybersecurity policies and regulations and laws in each country, also form a macroscopic perception of the regulatory stringency in each country, gain insight into the regulatory requirements in key areas, and clarify compliance insights

Reference Source: Roland Berger

Detailed Working Content of the Trends of Cybersecurity Situation in Various Countries

Mission 2: Trends of Cybersecurity Situation in Each Countries

Key problems to be researched in the project

Legislative and Supervisory Subjects and Management Structure

> What are the legislative and supervisory departments? What are the responsibility respectively?

> What is the management structure and organizational relationship between each legislative and supervisory body?

Eco-participants and Cooperation Pattern

> What are the related cybersecurity service providers, standards certification agencies? What other subjects are included?

> What kind of cooperation pattern should be between Huawei and those participating agencies?

The Demands of Each Subject of the Cybersecurity E-cosystem

> What are the concerns and pain points faced by the legislative and supervisory subjects? How to better comply with the regulatory trend?

> What are the key concerns and demands of the participants in the ecosystem? How to better construct industrial cooperation?

Methodology and Resources

> Roland Berger's past project experience

> External Expert Interviews

> Desk Research

> Official public Information of government and regulatory agencies

Working Purpose and Output Content

> The first purpose is to sort out the main body of legislation and regulation, clarify the management structure, and the development trend of its regulatory requirements which can help Huawei better comply with the regulatory requirements. The second purpose is to sort out the participating bodies of the cybersecurity ecosystem, clarify the cooperation pattern and key Appeal so that Huawei can better construct an industrial cooperation ecosystem.

Reference Source: Roland Berger

Detailed Working Content of the maps of the Cybersecurity Stakeholder

Mission 3: the Maps of the Cybersecurity Stakeholder

Key problems to be researched in the project

Sort Out the Key Figures of the Supervision Organization

> Who are the key figures in the regulator we need to focus on building collaborative relationships?

Sort Out the Key Figures of the Standard-Setting Agencies

> Who are the key figures in the standards-setting agencies and industry associations we need to focus on building collaborative relationships?

Sort Out the Key Figures of the Academic Community

> Who are the key figures in the standards-setting agencies and industry associations we need to focus on building collaborative relationships?

Sort Out the Key Figures of the industrial Circles

> Who are the responsible people in cybersecurity that we need to focus on among customers?

> Who are the key pfigures in other leading ICT companies we need to focus on building collaborative relationships?

Methodology and Resources

> Roland Berger's past project experience

> External Expert Interviews

> Desk Research

> Official public Information of relevant agencies

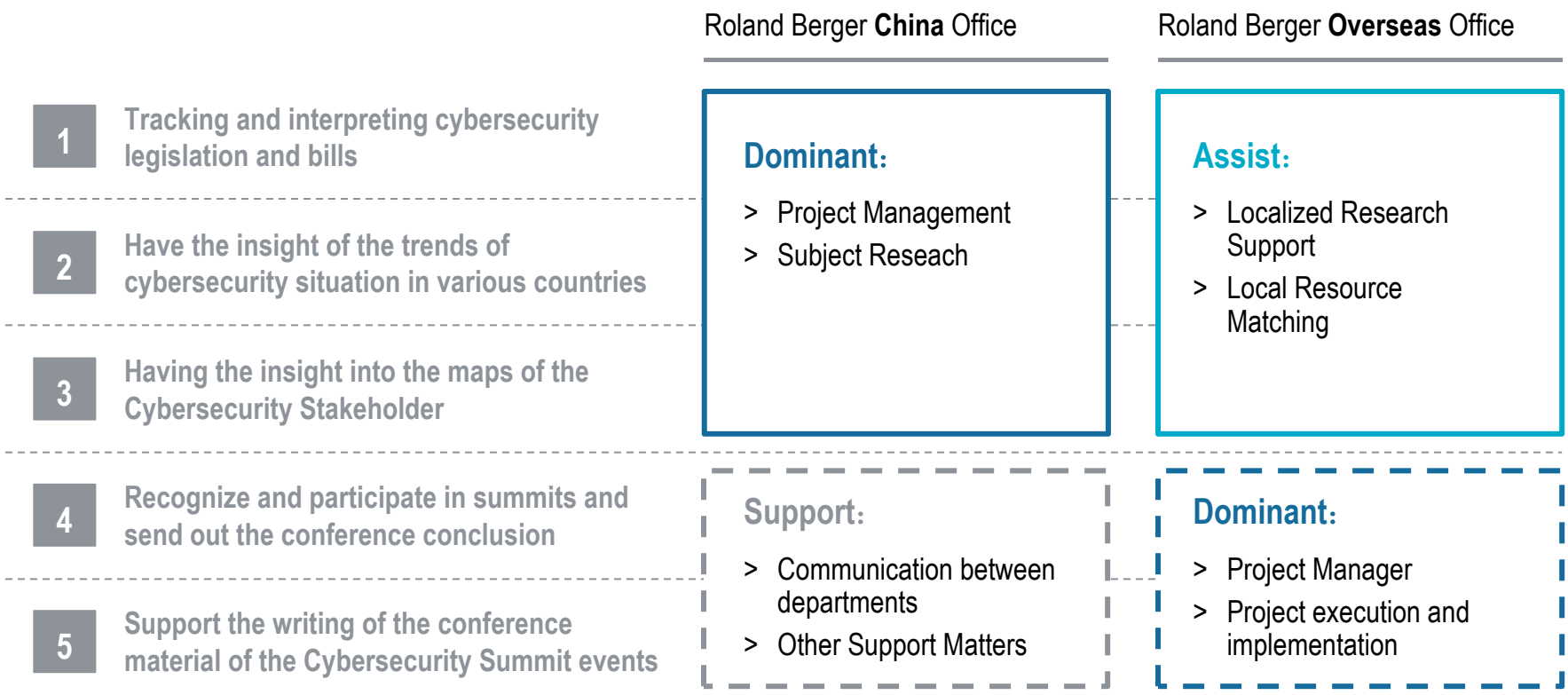
Working Purpose and Output Content

> The purpose is to sort out the list of people who need to focus on building relationships, and the list of key figures who can enlarge the voice of Huawei or help Huawei improve its cybersecurity capabilities

Reference Source: Roland Berger

Missions 1-3 will be led by the China office and supported by researchers from overseas offices as a team, Missions 4-5 will be led by overseas offices and internal communication are in process

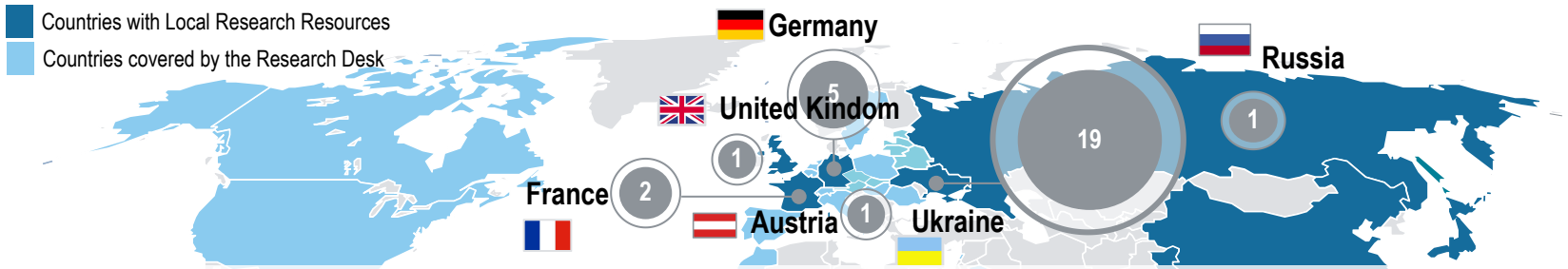
Division of Labor Between the China Office and Overseas Offices



Reference Source: Roland Berger

Roland Berger has more than 1,500 employees in 22 offices in Europe. In addition to front office consultants, We also have a European research competence Desk of about 20 researchers in Eastern Europe

Roland Berger Overseas Office and Research Desk



Headquartered in Munich

Amsterdam
Bangkok
Barcelona
Beijing
Beirut
Berlin
Boston
Brussels
Bucharest
Budapest
Casablanca
Chennai
Chicago
Detroit
Doha
Dubai
Düsseldorf
Frankfurt
Gothenburg
Guangzhou
Hamburg
Hong Kong
Jakarta
Kiev
Kuala Lumpur
Lisbon
London
Madrid
Manama
Milan
Montreal
Moscow
Mumbai
New Delhi
Paris
Pune
Riyadh
Rome
São Paulo
Seoul
Shanghai
Singapore
Stockholm
Stuttgart
Taipei
Tokyo
Vienna
Yangon
Zagreb
Zurich

Reference Source: Roland Berger

Out of 28 countries, our local consultants resources are able to cover a total of 5 countries including Sweden/Austria/Romania, and the actual research capacity is able to cover a total of 14 countries

Local Resources and Research Capabilities Coverage

Country	Status	Country	Status	Country	Status	Country	Status
SN1-Poland	√	SN2-Lithuania	√	SN5-Greece	✗	SN7-Urkraine	√
SN2-Sweden	√	SN2-Denmark	√	SN5-Bulgaria	✗	SN8-Serbia	✗
SN2-Norway	√	SN3-Czech Republic	√	SN5-Kosovo	✗	SN8-Montenegro	✗
SN2-Finland	√	SN3-Austria	√	SN5-Macedonia	✗	SN8-Hungary	√
SN2-Iceland	✗	SN3-Slovakia	✗	SN5-Albanian	✗	SN8-Croatia	√
SN2-Estonia	√	SN4-Romania	√	SN5-Cyprus	✗	SN8-Slovenia	✗
SN2-Latvia	✗	SN4-Moldova	✗	SN6-Turkey	√	SN8-Bosnia	✗

Local Reseources Covered
Research Capacity coverd
Unable to Cover

Reference Source: Roland Berger

We will adjust personnel input based on the actual needs of this project. The initially planned project team will consist of 5 Chinese office members and 2-4 overseas office members

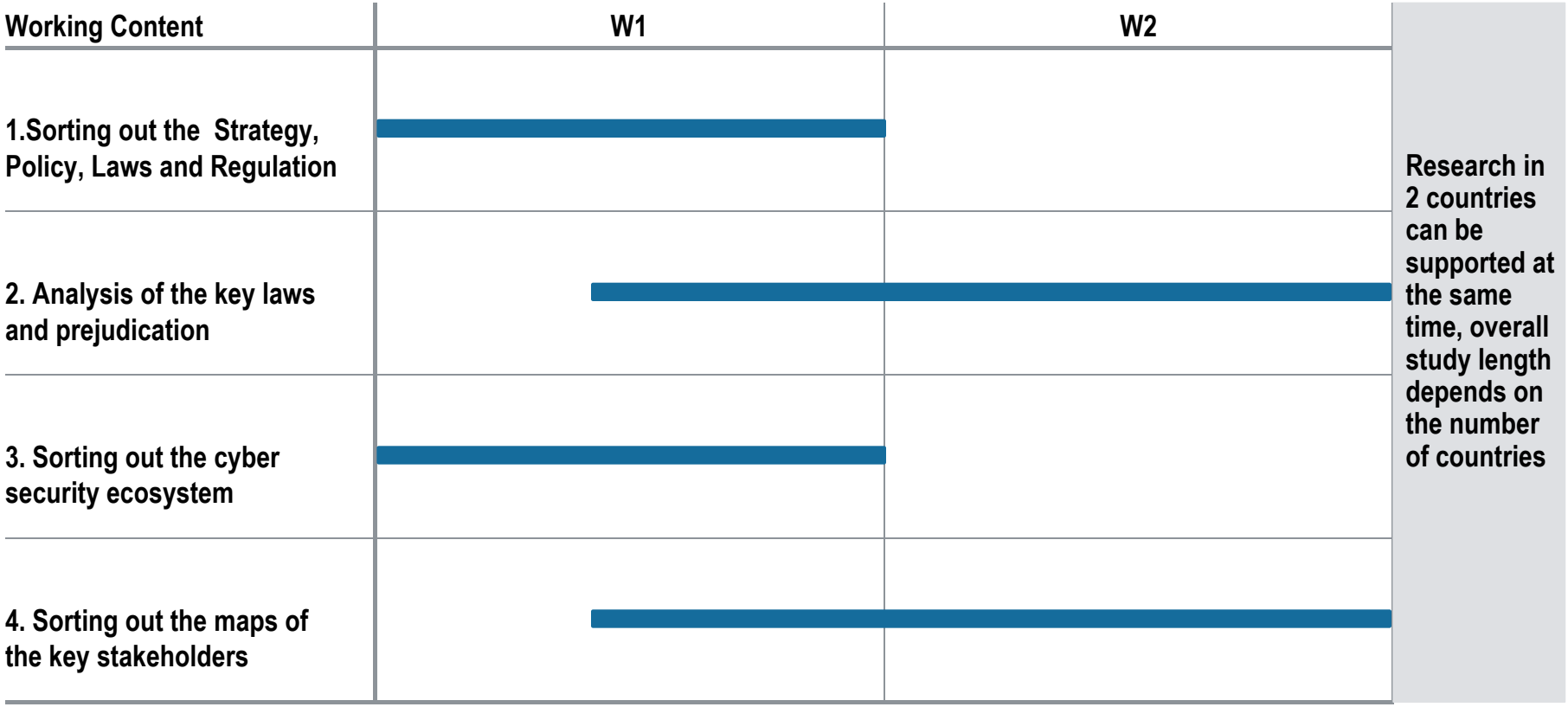
Personnel Allocation Plan

		Roland Berger **China** Office	Roland Berger **Overseas** Office
1	Tracking and interpreting cybersecurity legislation and bills	**Dominant Project:** > 1 Full-time Project Manager > 4 full-time consultants	**Auxiliary Study:** > 2-4 Full-time Researchers
2	Have the insight of the trends of cybersecurity situation in various countries		
3	Having the insight into the maps of the Cybersecurity Stakeholder		
4	Recognize and participate in summits and send out the conference conclusion	> Pending:	> Pending:
5	Support the writing of the conference material of the Cybersecurity Summit events		

Reference Source: Roland Berger

The research in two countries can be operated at the same time supported by the staffs in this project, with a preliminary estimate of 2 weeks to accomplish the research work for each country

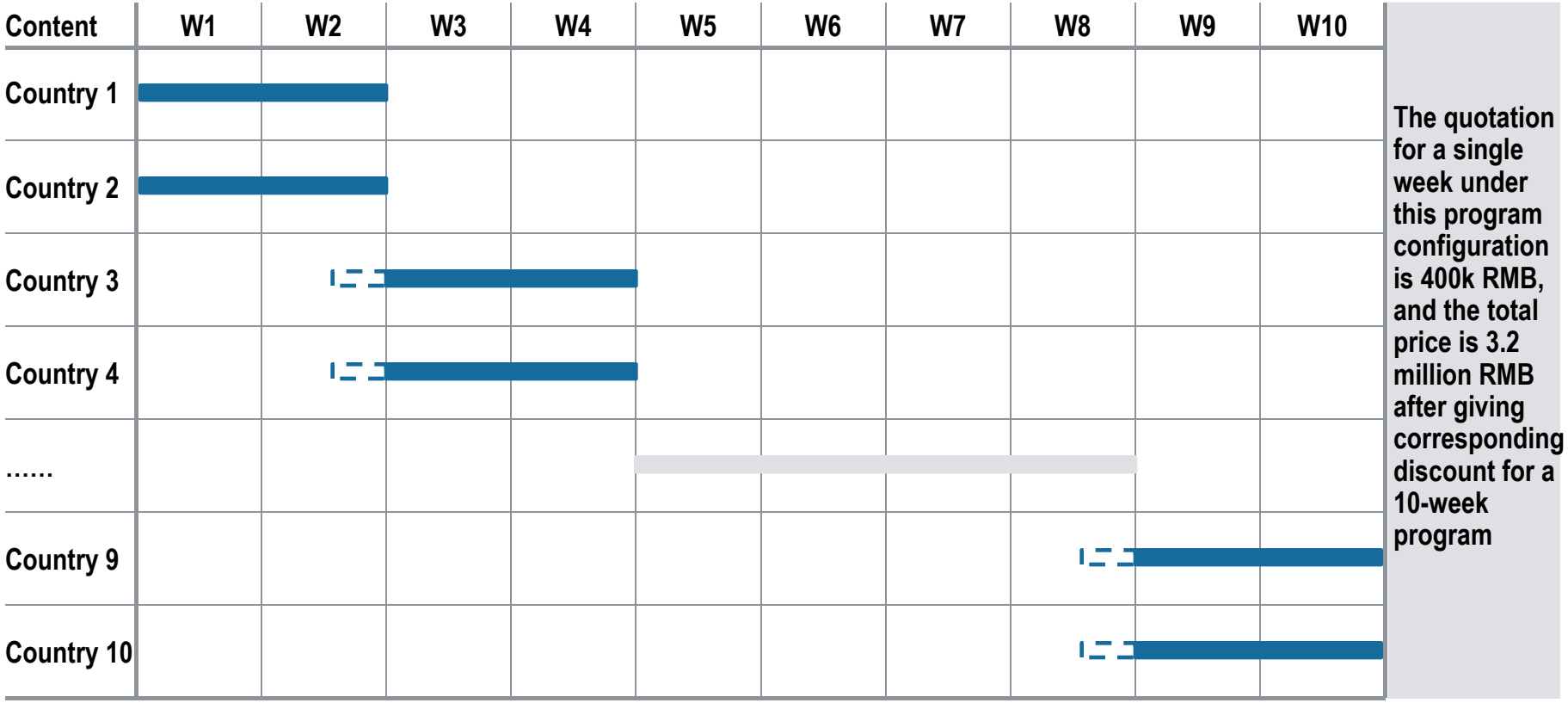
Working schedules for individual countries



Reference Source: Roland Berger

We recommend selecting certain countries as the first pilot projects. For instance, the overall implementation cyclef or 10 countries would be 10 months

Overall project duration and initial quotation



Reference Source: Roland Berger

We believe the project still has issues to be considered, including the business scope covered, batch priority for implementation, and some details of this project

The Problems We Suggested to Clarify

	Related Issues	Detailed Description of the Problems
1	**Scope of Coverage for Business**	> Since there are many industries involved in cybersecurity laws and regulations, it's necessary to study from the perspective of business needs, such as 5G devices and 5G toB/toC, new business in intelligent car cloud computing, the digital transaction for government and companies (financial/manufacturing/...), etc. > Conducting research on relevant laws, regulations and policies based on **strategy** and local **business needs**
2	**Batch priority of execution**	> For geopolitical reasons, the difficulty of compliance and the practical effects that compliance initiatives can bring vary greatly from different countries, while countries with similar economic, cultural, and geopolitical backgrounds have certain similarities for implementation so that we can research on those countries based on the similarities > Therefore, it is necessary to **prioritize** the execution of studies and **batches**: the cases with better results should be the priority, and the cases with similarities should be executed at the same time
3	**Detailed Requirements Content**	> Refinement of some of the requirements and clarification of the purpose, including: – The scope of content included in the **ecological trend**, and the purpose of the scan – Whether the **standard scans** need to be included – Whether the relevant policies and laws of **data security** need to be included

Reference Source: Roland Berger

B. Initial Understanding of the Porject Topics

For the topics covered in the project, we have considered the significance of the implementation for this project and initially sorted out the information

Project Preliminary Topics

1 Tracking and interpreting cybersecurity Policy and Regulation

- > Strategic positioning in cybersecurity in various countries
- > relevant policies about cybersecurity in various countries
- > Industry laws and regulations and precedents of various countries

- > Clear regulatory requirements
- > Sorting out the priority
- > Develop a implementation plan

2 Insight of cybersecurity trends

- > Relevant supervision and standard organizations
- > Other related industrial entities
- > Appeals of each industrial entity

- > Clarify the regulatory/participation body
- > Clarify the target of cooperation

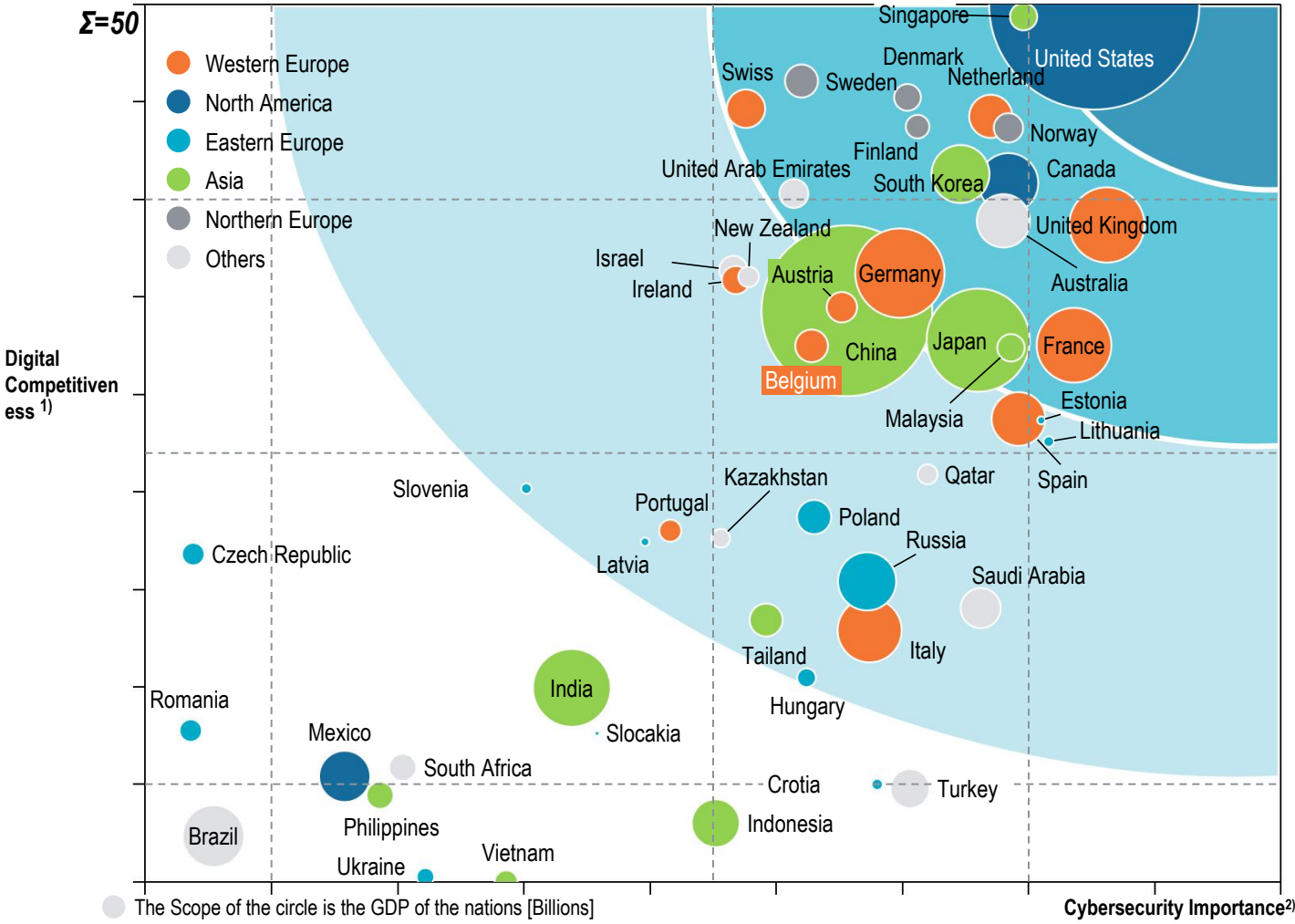
3 Maps of the cybersecurity stakeholders

- > Working groups and lead members of the various organizations
- > Maps of cybersecurity experts (KOL)

- > Seek partnership opportunities
- > Promote joint statement/endorsement

Reference Source: Roland Berger

Through a preliminary scan of global policies, four major ladder camps can be sorted out according to the importance of national digital competitiveness and cybersecurity, each with different demands to digital sovereignty



Leader Σ=1

> Technical protectionism
> Data long-arm jurisdiction
> National Security and Infrastructure Security

Pursuer Σ=16 (EU=8)

> Technical autonomy
> Data protectionism
> Rule-making and international order construction

Follower Σ=20 (EU=12)

> Market trade for technology, certain sovereignty gives up
> Relatively weaker cybersecurity concerns
> Following data policy and laws

Beginner Σ=13 (EU=4)

> Data protectionism
> Vulnerable countries in digital international games

1) IMD International Management Institute Global Digital Competitiveness Ranking 2019, Switzerland, including three dimensions of technology, knowledge, and future-proof readiness
2) International Telecommunication Union Global Cybersecurity Index 2018, including legislation, technical system, capacity building system, organizational system, external cooperation system five dimensions

Reference Source: IMD, ITU, Analysis from Roland Berger