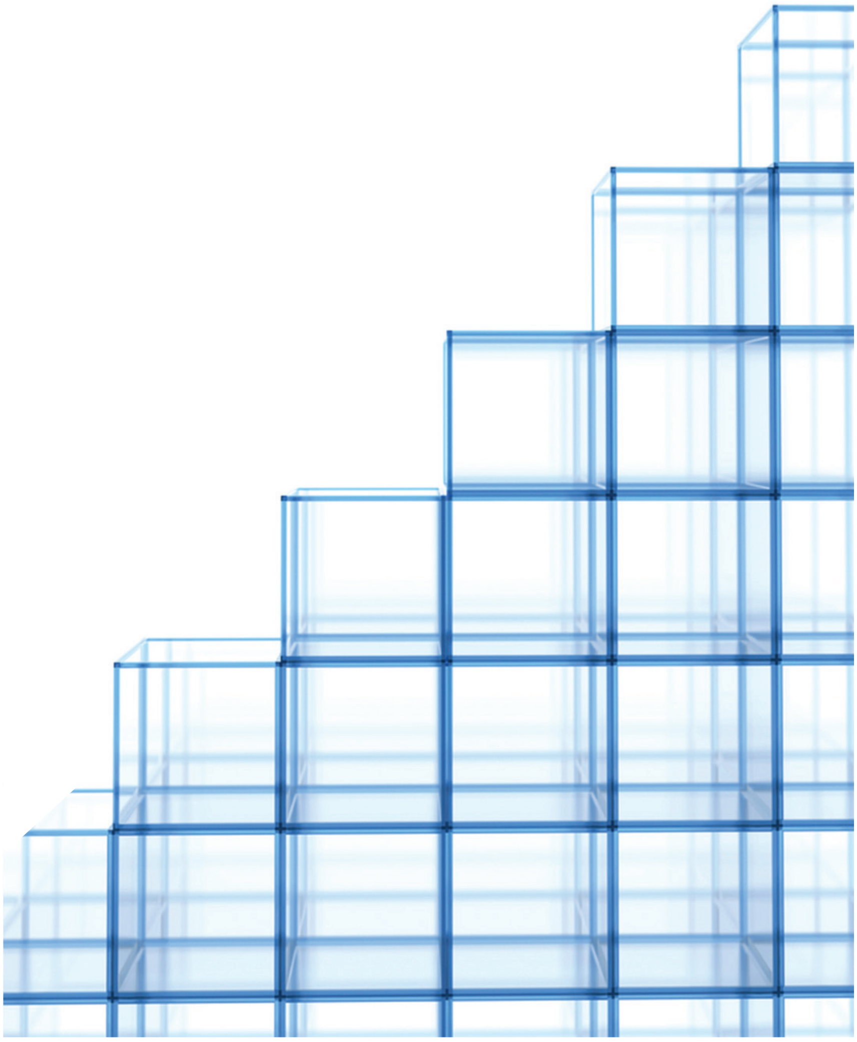
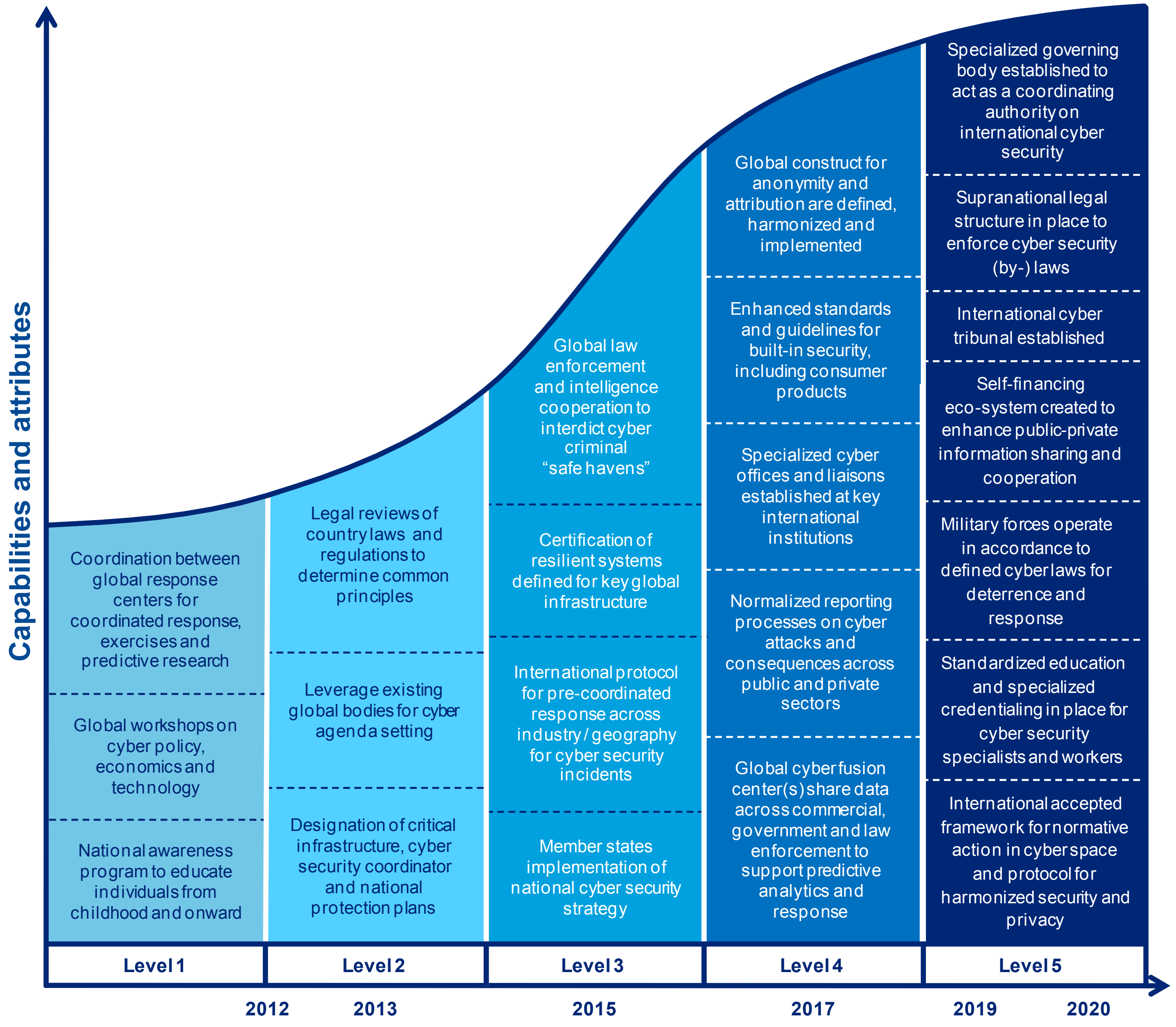
Deloitte.

Securing cyber space by 2020

A cyber security framework for global cooperation



Global cyber maturity curve: Collective action and milestones



Capabilities and attributes

Level 1

Coordination between global response centers for coordinated response, exercises and predictive research

Global workshops on cyber policy, economics and technology

National awareness program to educate individuals from childhood and onward

Level 2

Legal reviews of country laws and regulations to determine common principles

Leverage existing global bodies for cyber agenda setting

Designation of critical infrastructure, cyber security coordinator and national protection plans

Level 3

Global law enforcement and intelligence cooperation to interdict cyber criminal "safe havens"

Certification of resilient systems defined for key global infrastructure

International protocol for pre-coordinated response across industry/geography for cyber security incidents

Member states implementation of national cyber security strategy

Level 4

Global construct for anonymity and attribution are defined, harmonized and implemented

Enhanced standards and guidelines for built-in security, including consumer products

Specialized cyber offices and liaisons established at key international institutions

Normalized reporting processes on cyber attacks and consequences across public and private sectors

Global cyber fusion center(s) share data across commercial, government and law enforcement to support predictive analytics and response

Level 5

Specialized governing body established to act as a coordinating authority on international cyber security

Supranational legal structure in place to enforce cyber security (by-) laws

International cyber tribunal established

Self-financing eco-system created to enhance public-private information sharing and cooperation

Military forces operate in accordance to defined cyber laws for deterrence and response

Standardized education and specialized credentialing in place for cyber security specialists and workers

International accepted framework for normative action in cyber space and protocol for harmonized security and privacy

2012 2013 2015 2017 2019 2020

Protecting cyber space

Many governments understand that protecting cyber space is critical to the economic and national security of their countries. But unlike other domains of global relations, few rules govern interactions in cyber space.

Fast forward to 2020: A secure cyber environment

Imagine that, by the year 2020, we are operating in a secure cyber environment where the challenges we are experiencing today have been addressed. How did we get here? What did we do between 2010 and 2020?

This global cyber framework seeks to address some of these questions by proposing a maturity curve model as a guide for the international community to work together better to solve cyber security issues, such as addressing gaps in international law for pursuing criminals across borders, sharing information, and collaborating on incident response. The framework describes some of the steps that we believe may need to happen to develop a more secure cyber space by 2020, addressing key areas like the following.

Governance

Governance for cyber space includes global rules, treaties and protocols, similar to those in place for national defense, trade, and human rights.

Legal

Much cyber crime is transnational, and fighting it may require an international legal framework.

Technical

The rapid introduction of new technologies and increasing interdependencies across technologies, networks and applications underscores the need for tightening security for new technologies and establishing worldwide standards for security. Many organizations (commercial and government) may disagree.

Resources

The technology and managerial expertise of the workforce – including specialists who can address diverse issues including legal, intellectual property, and diplomatic challenges – and the "pipeline" of potential new talent will need to be increased, particularly with highly technical skill sets. In addition, information sharing and research and development resources will need to be put into place and funded.

Awareness

Cyber security cannot be achieved through technology alone. It requires a cultural understanding and a widespread willingness to demonstrate secure behaviors consistently.

	Governance	Legal	Technical	Resources	Awareness
Global and regional organizations	• Establish a coordinating agency • Develop international policy framework • Coordinate international approach and efforts on deterrence and incident response • Define global and regional responsibilities and alignment	• Formulate a structure to enforce cyber laws • Define normative behavior in cyber space • Establish proactive and preemptive cyber practices and protocols • Address the privacy issues associated with attribution	• Develop and establish technical standards and guidelines for secure products • Form public-private partnerships • Address the technical issues associated with attribution	• Set qualification standards for cyber security professionals • Make funding arrangements • Stimulate exchange of information	• Build commitment • Promote development of capacities • Sponsor cyber security programs
National governments	• Appoint a national coordinator and prepare a strategy • Incent (critical) industry security • Enforce information sharing on incidents	• Reexamine statutes governing investigations • Designate a privacy and liberties official • Create legal standards for securing critical cyber infrastructure	• Improve market incentives for secure and resilient hardware and software products • Establish standard certification metrics	• Incorporate education programs from early education on to expand and train workforce • Expand on research and development programs • Conduct initiatives to attract people to cyber security as a career	• Initiate public awareness and education program for children, adults, elderly, and others • Initiate national helpdesk for companies • Stimulate research and development
Private sector and industry	• Establish consultative structure to agree on sector/industry standards	• Sector/industry agree on legal standards for services and products	• Sector/industry agree on security standards for cyber security products	• Participate in national initiatives • Retool existing workforce	• Stimulate industries to educate the workforce, particularly in critical sectors

Contacts

General (ret.) Dick Berlijn
Senior Board Advisor
Deloitte Netherlands
dberlijn@deloitte.nl

Graeme Matthews
Partner
Deloitte LLP
gmatthews@deloitte.co.uk

Adel Melek
Partner
Deloitte & Touche LLP
amelek@deloitte.com

Lt. General (ret.) Harry D. Raduege, Jr., USAF
Chairman, Deloitte Center for Cyber Innovation
Director, Deloitte Services LP
hraduege@deloitte.com

JR Reagan
Principal
Deloitte & Touche LLP
jreagan@deloitte.com

Chris Verdonck
Managing Director
Deloitte Touche Tohmatsu Limited
cverdonck@deloitte.com

Ruud Vonck
Partner
Deloitte Netherlands
rvonck@deloitte.nl

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and deep local expertise to help clients succeed wherever they operate. Deloitte's approximately 170,000 professionals are committed to becoming the standard of excellence.

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this publication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this publication.