

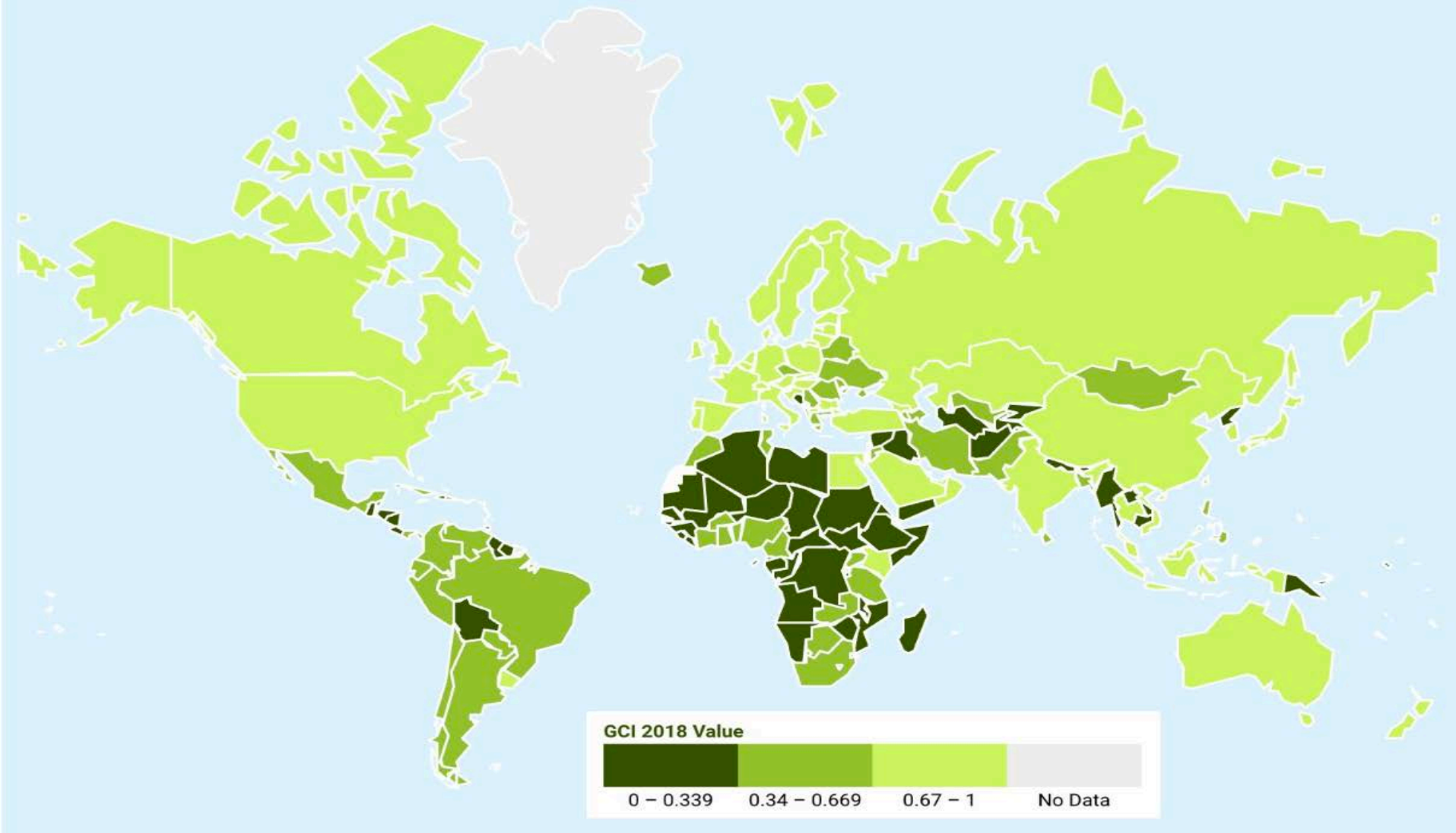
Introduction to the dimensions of digitalisation

Module 3.4 Cyber Security

Agenda

Module 3.4: Cyber Security

- Status-Quo
- Main threats
- Practical Guidance



ITU Global Cyber Security Index 2018

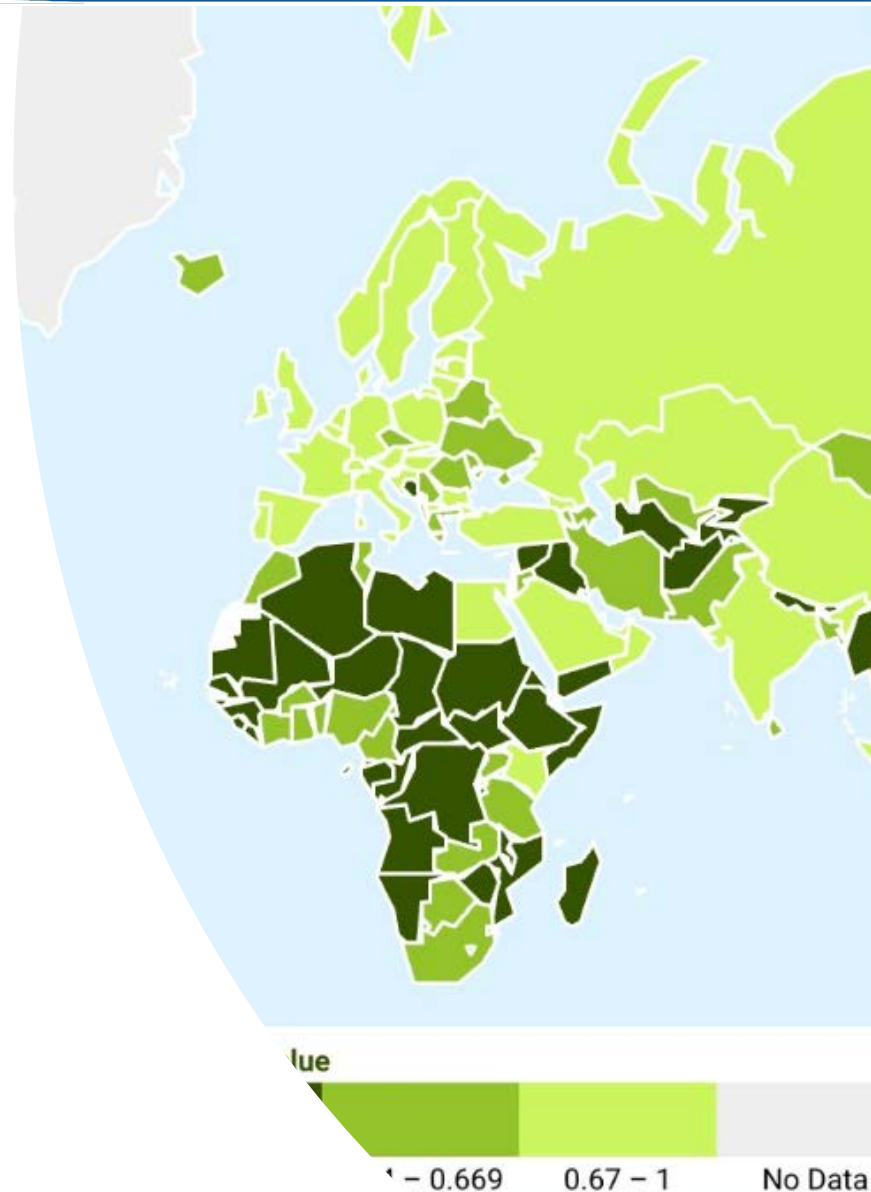
Heat map of national Cyber Security commitment

1.  Countries that demonstrate high commitment in all five pillars of the index.
2.  Countries that have developed complex commitments and engage in cybersecurity programmes and initiatives.
3.  Countries that have started to initiate commitments in cybersecurity.

Cyber Security

Status quo in Africa

- **Few governments** in the region have implemented national **cyber strategies**
- Only **20 percent** of the African states have implemented a **legal framework** for cybersecurity, and only 11 countries have enacted substantial laws to fend off cybercrime
- **Cybercrime** in Africa is becoming more sophisticated and creating **significant financial losses**: Cybercrime cost Africa an estimated US\$3.5bn in 2017



Cyber attacks are growing and become more sophisticated



Vulnerability and threats affect all stakeholders



Source of threat	Governments 	Private Organisations 	Citizens 
Professional criminals	Disruption of IT Manipulation of information Theft and publication or selling of information IT takeover	Disruption of IT Manipulation of information Theft and publication or selling of information IT takeover	Disruption of IT Manipulation of information Theft and publication or selling of information IT takeover
State actors	Digital espionage Offensive cyber capabilities Theft and publication of information	Digital espionage Offensive cyber capabilities Theft and publication of information	Digital espionage
Terrorists	Disruption/Takeover of IT	Disruption/Takeover of IT	Theft and publication of information
Cyber vandals and script kiddies	Theft of information Disruption of IT	Theft of information Disruption of IT	Theft of information
Hacktivists	IT Takeover Theft and publication of obtained information Defacement	IT Takeover Theft and publication of obtained information Defacement	IT takeover
Internal actors	Theft and publication or selling of obtained information Disruption of IT	Theft and publication or selling of obtained information Disruption of IT	IT takeover
Private Organisations		Information theft (industrial espionage)	Commercial use/abuse or "resale" of information
No actors	IT failure	IT failure	IT failure

Cyber Security: a real thing in agriculture sector too!

THE WALL STREET JOURNAL

Subscribe | Sign In

Home World U.S. Politics Economy Business Tech Markets Opinion Life & Arts Real Estate WSJ Magazine



TECH

Agriculture Giants Boost Cybersecurity to Shield Farm Data

Companies like Monsanto and Deere invest more as business becomes more datacentric

By Jacob Bunge

Feb. 19, 2015 4:08 pm ET

ARLINGTON, Va.—Agriculture companies are building sturdier digital fences to fend off cyberattacks that industry officials say are increasingly targeting the sector.

Companies including [Monsanto Co.](#) and [Deere](#) DE 1.46% & Co. are investing more in cybersecurity as the farming business grows more datacentric, with satellite-steered tractors and algorithm-driven planting services expanding across the U.S. Farm Belt, executives said at an industry event Thursday.

Dell: Security key for IoT in agriculture

Exec says agriculture already embracing IoT, but obstacles remain

By Sharon Harding | Public Sector | 19 May 2015

What is the Cybersecurity Threat in Agriculture?

September 28, 2016 Lauren Manning

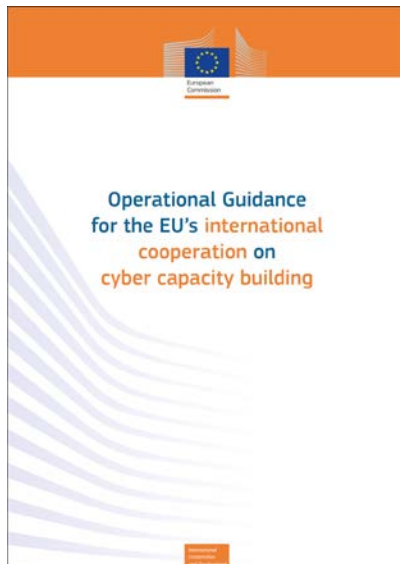
There is a whole lot of data being compiled in the agriculture space. In agtech circles, the discussion has typically centered around how to process this data to provide farmers with timely, actionable insights. There's

What cybersecurity challenges do farmers face?

The four areas that present a cybersecurity threat in agriculture are in access to services, personal privacy areas, proprietary information, and IP. As I tell my clients, the trust in the food chain starts in the dirt and ends on the table. While you can probably say that the probability is not zero in any of those categories for any part of the ag business, it is more about the various combinations of these four categories.

Cyber Security

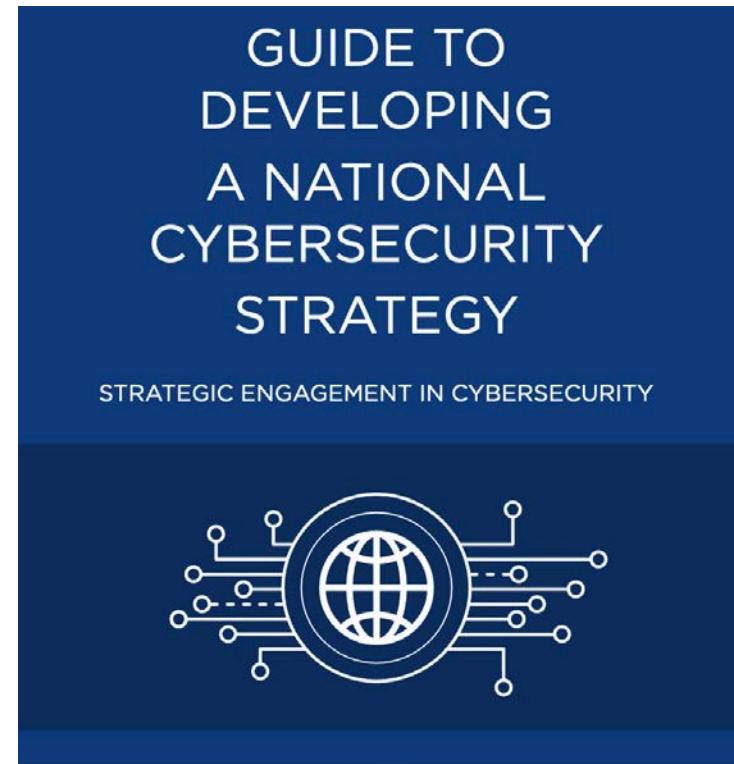
Key stakeholders



Designing Cyber Security Measures: Helpful Guidance



Operational Guidance
for the EU's **international**
cooperation on
cyber capacity building



Cyber Security

Group discussion: Country assessment

What is the current state of discussion on cyber security policy in your country?

- What are the major threats?
- What are the policy objectives?
- What are the existing institutional capacities?



10 min