

Resilient Digital Civilisation

Contributions from the Working Group on Secure ICT - Research and
Innovation of the NIS Platform



7 - 8 April 2014
Vienna, Austria



- The Main focus of this Aol is the protection of the groups/society/organizations (we will call this ‘Digital Interconnected society’ as it represents the collective interest of the organized citizens, institutions, etc.);
- Focusses on the institutions of society, i.e. the organisations that make up our government, business, and civil society, which increasingly rely on digital technologies to operate, offer services, and interact with citizens, with customers and with each other;
- Aims to identify the challenges, issues and risks that organisations face in a digital ‘interconnected society’ and to identify the technologies and approaches to ensure that they can be trusted, secure, and can meet the obligations imposed on them by society, whilst at the same time benefiting from innovative technology and services.

Aol#1: Citizen Digital Rights and Capabilities (Individual layer): ensuring that, as ICT is used by people, it addressing rights, needs, wants of citizens as individuals – in a sense this looks at the trust problem from the ‘demand side’. Citizen’s rights and needs and wants (rights and societal norms) have to be met by the organisations as to how they behave online, the risks they are exposed to and how they use and manage digital data.

Aol#2: Resilient Digital Civilisation (Collective layer): Digital Interconnected society – ensuring that digital institutions of society are as trusted in their digital forms as they are in physical form, in a way this is the ‘supply side’. Organisations operate under a whole series of obligations – regulation, contracts, societal norms, and to manage risks, ensure security, and handle information securely and respecting fundamental rights of the customers/citizens.

Aol#3: Trustworthy (Hyperconnected) Infrastructures (infrastructure layer): ensuring security and continuity of infrastructures and systems – so that the economy and institutions can operate. Infrastructures and systems need to be secured against threats and failures to ensure the continuity of institutions and services they support.

- Digital Civilisation is a fact
 - Media, social relations, critical infrastructures, services, surveillance, industrial control, government, smart cities, ...
- Digital civilisation is desirable
 - Ease, convenience, economisation, speed, information access, optimisation, proximity, ...
- Digital civilisation is exposed to new threats
 - accessibility, invisibility, profiling, connectivity, complexity, ...
 - Shared platforms and infrastructures increase impact of incidents,
- Resilience is key for a functional digital civilisation
- Ability for each individual and entity to manage and balance their risks
- Do concepts and solutions of the “analog” world scale?

Technical

- Interoperability
- Adaptation
- Security metrics
- Trust & assurance
- Security engineering
- Security & privacy by design

Political / Societal

- Diversity
- Policy & regulation
- International aspects
- Values and rights
- European view
- Data protection principles
- Framework (certification etc.)

Economical

- Economic value of security
- Large-scale coordination
- Transparency of business models
- Bid players -- SMEs
- Scale, complexity

Educational

- Awareness
- Multi-disciplinarity
- Risk perception
- Ease of use
- Simplicity

Enablers (of 36)

- Automation
- Privacy-friendly technology
- Risk management
- Secure Cloud
- “good enough” security
- Transparency
- Industry participation / PPP
- European expertise
- Education
- Case studies

Technology, policy, regulation

Inhibitors (of 25)

- Market fragmentation
- Security seen as cost driver
- Lack of awareness
- Complexity
- Reluctance to share information
- Privacy risks
- Reactive approach

Mostly non-technical

Gaps identified

- Business and governance models
- Risk models
- Scalability and cost-effectiveness
- Privacy and security by design, including consumer products
- Strong end-to-end assurance, trustworthy systems
- Simplification, lightweight approaches, usability
- Information collection and exchange
- Metrics and measurement
- Empowering citizens
- Global standards
- Multi-disciplinarity



Trust
In The
Digital
World

7 - 8 April 2014
Vienna, Austria



TDL | Trust in
Digital
Life

Contact: JimClarke, WIT, jclarke@tssg.org
Nick Wainwright, HP Labs, nick.wainwright@hp.com