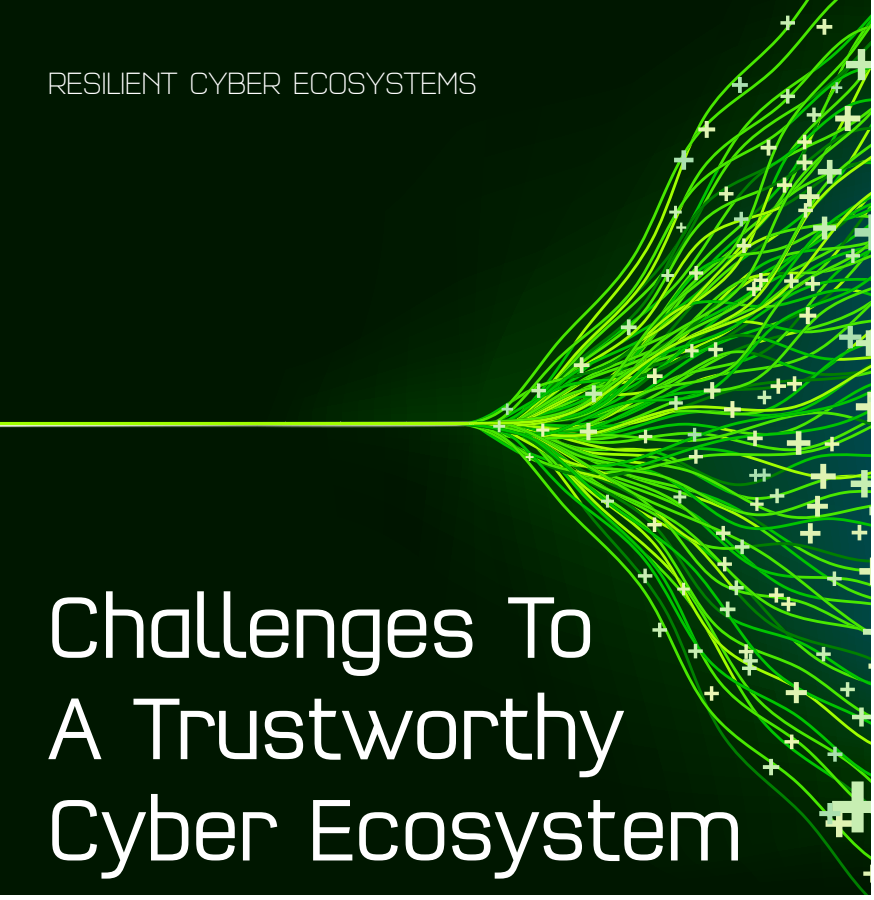

# Challenges To A Trustworthy Cyber Ecosystem

**Ian Bryant,** De Montfort University, Leicester, UK
**Jasvinder Mahrra,** Institute for Security and Resilience Studies, UCL, UK

**Abstract.** Cyberspace is recognised as the first man-made environment. Like other natural environments it cannot be controlled. Cyberspace, of which software forms an intrinsic and indivisible element, is ever evolving and an ever growing dependency for defence, yet is contingent upon a variety of diverse participants—private firms, non-profit organisations, governments, individuals, processes, and cyber devices. It is therefore vital that intrinsic challenges to cyberspace—and software—are recognised and treated such that a trustworthy cyber ecosystem can be formed.

## The Cyber Ecosystem

Cyberspace is now acknowledged to be the first man-made environment on par with air, land, maritime, and space. Indeed, it weaves all these environments together as never before. Yet, much like these other natural environments, it cannot realistically be controlled.

In doing so, cyberspace does not erase spatial boundaries—rather the transnational dimension opened up by cyberspace allows for anonymity. In contrast to the eons of time the sea has affected life on earth, cyberspace has infiltrated the whole ecosphere in decades. This constantly evolving environment is an emerging national security challenge to all nations. Indeed, the U.S. International Strategy for Cyberspace (May 2011) [1] reported, "Unauthorised network intrusions threaten the integrity of economies and undermine national security." It saw the need for collaboration between the public and private sector as crucial to protect the innovation and secure critical infrastructures such as energy, transportation, finance, and the defence industrial base, central, and local government. The problem of security is inherently complex involving not just national security concerns but commercial interests and privacy.

These characteristics challenge the defining assumptions that underpin conceptions about competent authority, jurisdictions, conflict, criminality, cash, and the use of force. The physical movement of troops through a neutral state's territory would violate neutrality. However, the same is not true for any cyber violation in which communications can pass through another state's infrastructure. How to handle cyber issues is becoming of strategic importance for governments worldwide as they strive for trustworthy and reliable networks.

Protecting the infrastructure becomes all the more essential against the impacts of disruptions and cyber attacks because the forces at work in cyberspace may more readily be asymmetric, that is, unconventional and disproportionate. So far, the new environment has demanded immediate responses, based on inherited tools or technological innovations as we progress. However, these may be necessary but are not sufficient by themselves as they offer only short terms, partial remedies.

Trustworthy cyberspace is vital to the prospects of enhancing a government's reputation for trusted and reliable hubs and networks, but the evolution of cyberspace is uncertain. Conventional approaches to this new ecosystem will not be sufficient and require a new ethos and culture of thinking. Whilst cyberspace can promote freer markets, the proliferation of some knowledge will need greater care. Cybersecurity experts themselves are calling for a radical change of ethos [2].

Whilst there has been a convergence of telecommunications, computer processing and interactive multi-media content, technological convergence is far from complete. Developments of cyber, bio, and nanotechnology are morphing into one another, and the boundaries between users and developers is blurring. But the future lies in cyberspace, and this needs to be trustworthy.

## Cyberspace and Software

It is difficult to conceive of any major sector of the economy in the developed world that is not dependent (often critically so) on Information and Communications Technology (ICT) and software. This dependence extends into our private lives; with figures for the UK in October 2011 showing that more than 50% of the population now has a smartphone.

This need for trusted, correct, and reliable operation requires that software be trustable, both in terms of its resistance both to accidental or collateral faults (as exemplified by, but not restricted to, the niche "safety critical" approaches), and to malicious acts (as exemplified by the "security" approaches). This applies both to software and systems developed for specialist markets where trustworthiness is an explicit Functional Requirement (FR), and to all other software and systems, for which trustworthiness is an inherent but often forgotten implicit Non Functional Requirement (NFR).

The difference between these two views of trustworthiness is typically a matter of degree, with those for where these properties are a FR normally having Pareto or comprehensive assurance needs, whereas in the NFR space this is more likely to be a need for due diligence.

## Emerging Challenges

The 2010 UK National Security Strategy [3], as approved by the Ministerial National Security Council, identified 15 priority risks across the spectrum of national security risks to the UK. Of the four Tier One risks identified as being of particular concern, one is enumerated [4] as hostile attacks upon UK cyberspace, potential shortcomings in the UK's cyber infrastructure, and the actions of cyber terrorists and criminals: to which end a National Cyber Security Programme [5] has been created.

To address this risk requires a holistic view of the adversities that need to be addressed, as this needs to address both threats (deterministic, deliberate impacts from attacks by hostile actors) and hazards (stochastic, undirected impacts from either natural events and/or collateral damage from other hostile activities). An adversity-driven approach means that not only does an organisation need to understand the threat actors it faces (be they nation states, empowered small agents or cyber-criminals), but also to have an actuarial view of the likelihood of occurrence of other events, such as the chance of climatic or geologic problems causing loss of facilities or communications, or of loss of service from a distributed denial-of-service attack on a completely unrelated organisation with whom bandwidth is shared.

The diverse nature of adversities faced by the cyber ecosystem is in direct conflict with the way in which organisations and nations are normally structured, which historically and continues to be in isolated, and sometimes mutually competitive silos. Taking a nation-state approach as an example, the issues of foreign national-state attacks will typically be handled by the defence/security/intelligence community, the issues from cyber-criminality by the law enforcement/criminal justice community, and the issues from natural hazards by the civil contingency community. Organisations suffer from similar silo effects, with differential degrees of sharing of vital information with governments and their peer community.

The scale of challenge presented by software failures cannot be underestimated, with numerous studies [6][7] identifying problems with software as a major source of project failures, with high costs to the economy, enumerated by NIST as being about $60 billion per year to the U.S. alone, with no definitive figure currently being available for the UK or worldwide.

**This dependence of ICT and software can be expected to broaden and deepen in the coming years, with a number of trends already being identifiable to catalyse this dependence and complicate the problem space, including:**

- The move to distributed application platforms and services (a.k.a the cloud), where the boundaries of organisation and/or national jurisdiction are increasingly blurred, and the options for either proactive controls and/or reactive measures are similarly constrained.
- Increasing reliance on mobile devices, such as smartphones and tablets, which typically rely on lightweight operating systems with less inherent controls than operating systems of previous generation desktop devices.
- A move in business to consumerization and Bring Your Own Device, where the boundary of ownership is blurred between the organisation and the individuals who work for the organisation.
- Commoditisation in previously closed architectures, such as industrial control systems where, for instance, a step change is being encountered of previously bespoke sensor devices with wireline connections to proprietary control systems are being replaced by configurable, off-the-shelf sensors using wireless connections to generic ICT systems that have onward connections to the global internet.
- The pressure for ICT consolidation for energy efficiency for green reasons (the low carbon imperative) leading to extensive use of software virtualisation to separate previously physically distinct services.

**Furthermore, the way in which systems are developed and deployed is changing, with the historic assumption of ICT being engineering artifacts under single organisational control being subverted by factors such as:**

- The adoption of open source models for sourcing software, fundamentally disrupting views of single organisational control.
- The growth of multicore processor technologies, which can subvert the risk modelling approaches used in previous generations of hardware.
- Growing questions as to whether hardware platforms used for software can be trusted to execute as expected, with evidence of counterfeit hardware being found in multiple market segments.
- A blurring of the boundary between software and hardware boundary, for instance with the use of software style design languages to implement application-specific integrated circuits and field-programmable gate arrays.
- The increasing use of generic, self-documenting structured data (e.g. XML) to control systems' behaviours rather than rely on pre-defined execution paths.

**In terms of software development itself, the classic waterfall model of software development is evolving in a number of ways:**

- The adoption of other approaches such as agile and rapid application development by the software industry.
- The growth in small-scale software development, typically carried out by micro-business who will not invest in formal development approaches, as exemplified by the apps movement for smartphones and tablets.
- A plethora of activity which produces artifacts that have the properties of software, as exemplified by the mass of websites which use, to a greater or lesser extent, mobile or active code (such as Java, Javascript and ActiveX). In these cases many of the users will have little, if any, awareness that they are implicitly creating software functionality by their often point-and-click activities.

## Creating Trust

These uncertain developments require, "security and resilience for cyberspace to be seen as not just a service but are the services underpinning trust and confidence in an environment that touches all others" [8].

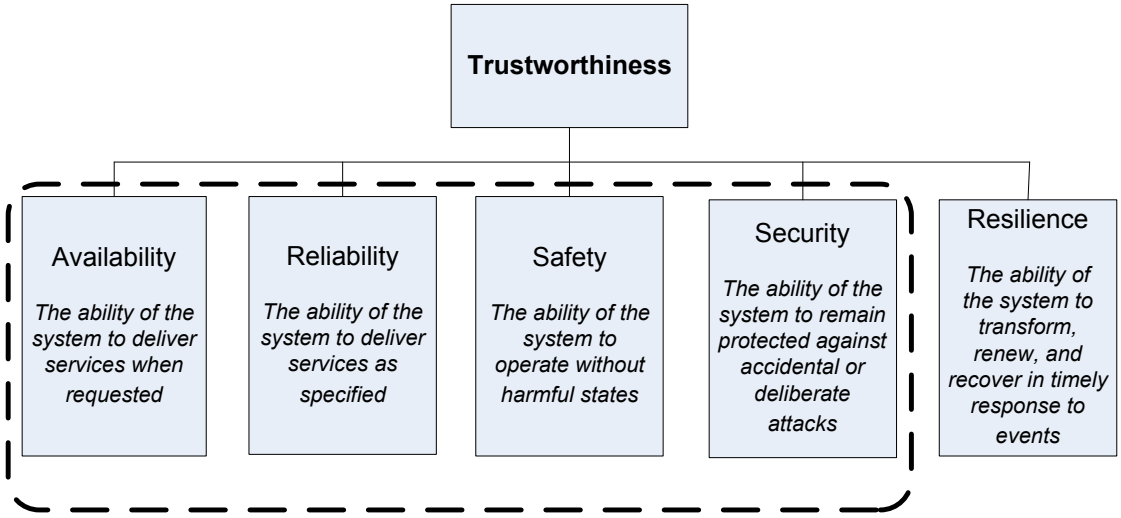


*Figure 1*

Security and resilience are defined [9] as being complimentary practices required to manage relevant aspects of an organisations operational risk, and have a number of competing definitions, of which the most useful are probably [10]:

- **Security:** the preservation of confidentiality, integrity, and availability of entities.
- **Resilience:** the property of an entity to transform, renew, and recover from the impact of interactions or events.

Investment in cyberspace protection must be increased if we are to move from seeing security as an organisationally focused afterthought and moving towards a more inclusive concept of resilience that is fit for our times, which needs to include consideration of all external and infrastructure dependencies, and the sets of both proactive and reactive controls needed to mitigate risks from such dependencies. It is about transformation first and not about cleaning up after the fact; not bouncing back but bouncing forward and learning to thrive on uncertainty.

But neither security nor resilience gives us holistic trustworthiness, and thus a more expansive model is needed.

Figure 1, adapted from previous work by Professor Ian Sommerville at St. Andrews University [11] attempts to link together the set of existing stovepipes of activity that need to be considered.

Thus in order to get the best from cyberspace and minimize the inherent dangers we need a holistic, ever vigilant, and innovative, approach to trustworthiness:

"A sustainable and trustworthy cyberspace will derive from open sources and standards, driving an internationally coordinated approach to research and development [7]."

## Delivering Trust

Whether the focus of concern is the organisation or the nation state, a successful protective regime should regard all adversities holistically so that the most pragmatic, appropriate, and cost-effective treatments can be applied and trustworthy solutions delivered—the option sets available against denial-of-service whether it be from an attack or a natural disaster are likely to be very similar.

Software represents a microcosm of the overall cyberspace, and therefore software engineering must attempt to escape a threat-driven mindset, addressing all adversities to deliver trust.

## ABOUT THE AUTHORS

**Ian Bryant** is the Technical Director for Software Security, Dependability and Resilience at the Cyber Security Centre, De Montfort University, Leicester, UK, where he is on academic attachment from the UK Ministry of Defence. He has more than 20 years of experience in information systems security, dependability and resilience across a number of public sector bodies, and is an active contributor to a variety of standards development organisations in both information security and systems/software engineering.

**E-mail: ib@dmu.ac.uk**

**Jasvinder Mahrra** is the Senior Research Fellow at the Institute for Security and Resilience Studies, University College, London, UK. She has more than 10 years of experience in resilience planning and exercising. Before joining ISRS she had her own consultancy and prior to this was part of the UK's Civil Contingencies Secretariat (Cabinet Office) coordinating a programme of events to enhance resilience and preparedness.

**E-mail: j.mahrra@ucl.ac.uk**

## REFERENCES

1. The White House; International Strategy for Cyberspace: Prosperity, Security and Openess in Networked World (May 2011)
2. Evans, K & Reeder, F; A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters, A report of the CSIS Commission on Cybersecurity for the 44t h Presidency, CSIS: Washington DC (2010)
3. Cabinet Offices; A Strong Britain in an Age of Uncertainty: The National Security Strategy; Cmd7953, Cabinet Office (October 2010)
4. Cabinet Office; Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review; Cmd 7948; Cabinet Office (October 2010)
5. Downing, E; Cyber Security – A new national programme; HC/SN/SC/5832; House of Commons (23 June 2011)
6. Flyvbjerg , B and Budzier, A; Double Whammy – How ICT Projects are Fooled by Randomness and Screwed by Political Intent Alexander; University of Oxford Saïd Business School / McKinsey (2011)
7. Standish "Chaos" Reports (2004 onwards)
8. MacIntosh, JP, Reid J & Tyler, L; Cyber Doctrine: Towards A Coherent Evolutionary Framework for Learning Resilience; Institute for Security & Resilience Studies, UCL (2011)
9. HM Treasury; Management of Risk - Principles and Concepts; HM Treasury (Oct. 2004)
10. ISO/IEC 27000; Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary; ISO/IEC (Working Draft March 2012)
11. Sommerville, I; Software Engineering (9th Ed.); Pearson (2009)