UK COMPUTING RESEARCH COMMITTEE

UKCRC response to Royal Society cybersecurity call for evidence

The UK Computing Research Committee (UKCRC), an Expert Panel of BCS The Chartered Institute for IT, the Institution of Engineering and Technology and the Council of Professors and Heads of Computing, was formed in November 2000 as a policy committee for computing research in the UK. Its members are leading computing researchers from UK academia and industry. Our evidence reflects the experience of researchers who each have an established international reputation in computing.

Research challenges

The academic response to the various initiatives that have been launched as part of the UK's cybersecurity programme, which has included the recognition of 11 Academic Centres of Excellence in Cyber Security Research, is an indication of the strength and breadth of cyber security research in the UK. Each of the centres had to demonstrate a substantial track record (publications, PhD graduations and funding) and a future vision. Each centre has a particular focus and these range from security infrastructure to safeguard the trustworthiness of information to the engineering of secure software systems. Subsequent funding initiatives have seen the creation of 3 Research Institutes, a programme of work to foster collaborations between scientists, technologists and social scientists (CERES) and between universities and business (BACCHUS). These various initiatives have been a good first step in creating a large and well-connected cybersecurity community in the UK.

In parallel to these Government and RCUK funded activities there a number of initiatives in big data and "data sciences". Some of these are funded through programmes such as the RCUK Digital Economy programme but some are directly funded through companies.

There has been research on security economics (e.g., pursued by Cambridge) as well as privacy economics (e.g., pursued by Carnegie Mellon University), both establishing links between security and privacy and the socioeconomic context. It is true for both security and privacy, that they are externalities and, thereby, discounted in system design. Security-by-design and privacy-by-design aim at integrating these properties in the system design process but are still at an early stage of development.

Europe has been investing over multiple years in privacy in its wider socioeconomic context, pursued in a series of EU Integrated Projects, starting with PRIME, over Primelife to ABC4Trust and FutureID. These projects gravitate around identity and privacy-enhancing technologies, yet consider the socioeconomic context, as well. Whereas existing research often focuses on point solutions for privacy-enhancing technologies and institutional privacy (e.g., with privacy paradigms such as k-anonymity or differential privacy), there is a need to integrate the strands of user privacy, institutional privacy and privacy-enhancing technologies to establish solutions that are socioeconomically viable. Moreover, there is still work to be done to develop better mechanisms, possibly bio-based, for authentication and identity management.

More generally, the application of bio-inspired technologies to cyber security and sustainability of the internet has not, as yet, received much attention from the UK research community. There has been work on applying techniques from epidemiology to model the propagation of computer viruses.

Cyberphysical systems (CPSs) have been the subject of major research programmes in the US (see cps-vo.org). Europe is beginning to invest in research in the area, with significant programmes in Germany (the acatech position paper was seen as particularly influential in this regard: www.acatech.de/cps). There is activity in the UK in this area (for example, in the Centre for Software Reliability at City University) and it is an area that is likely to become more prominent in the future. CPS are seen as the basis of Industry 4.0 (http://www.bmbf.de/en/19955.php), and there is a significant programme expected in the area in Horizon 2020. Cybersecurity of CPSs poses technical challenges related to both the character of CPSs as systems of systems and the interaction between cyber-side technology and the physical environment. These range from the provision of privacy in such heterogeneous networks to the integration of semantically very different models (e.g., how would a specified form of attack on a cyber-side network affect the power supply or water flow?). Such research requires multidisciplinary teams covering cyber-side, network and big data expertise with researchers from quite different disciplines, including for example mechanical and civil engineering, sensor technology, transport, etc. Cybersecurity of CPSs poses socio-technical challenges, in part because of the heterogeneity of CPSs, the data that may flow across multiple platforms and the extent to which users can understand and give meaningful consent to the use of data gained through CPSs, e.g. in health monitoring.

In the context of safety critical software systems there are major technical issues still to be addressed. It is difficult to update anti-viral systems to reflect new threats and at the same time meet the verification requirements of safety-critical software standards. Similarly, regulators are often unsure how companies could demonstrate that they are safe to resume operations once a safety–critical system has been compromised – given that testing techniques cannot guarantee that malware is *not* present. At the same time, we are facing new challenges from the development of pan-European infrastructures across both power and transportation infrastructures, for example under the Single European Skies programme. This creates new potential vulnerabilities through data exchange across national borders. These initiatives not only create technical challenges; they also lie at the intersection of research and policy in areas that have not yet received significant attention.

International collaboration

The FCO-funded Global Cyber Security Capacity Building Centre aims at sharing good practice. The main focus for this should be on the UK's main trading partners (now and in the future) and these are a good source of potential collaborators. At the present time the focus is on South East Asia (especially South Korea and Singapore), Europe and the US. Over the next 5-10 years sub-Saharan Africa and South America are likely to become more important. Already the FCO (via SOCA, now NCA - National Crime Agency) has supported cybersecurity partnerships with African countries, particularly those judged to be areas from which a lot of cybercrime is planned and coordinated. For example the OU have a UK-Ghana partnership funded by the FCO working with Ghanian universities on both cyberscurity education and targeted research activity (e.g. digital forensics).

Within Europe, the Horizon 2020 Societal Challenge on Secure Societies offers a mechanism for promoting collaborations. The various Broad Agency Announcements (BAAs) from US Agencies provide an opportunity to support collaborations between UK and US universities and industries. Since many of the leading cyber security companies are US but with a European base (e.g. McAfee, Symantec, etc), both funding schemes are relevant. Many countries also have special research programmes in cyber security (e.g. DFG in Germany, CNR in Italy) and the UK should make more effort to create better linkage with these.

We do not perceive a coordinated approach to security, privacy and trust in its wider socioeconomic context in the UK. In the EU and world-wide, there are initiatives towards security-by-design as well as privacy-by-design to be the basis for building systems. For security-by-design, we perceive the German institute CASED at TU Darmstadt as one of the European focus points. Research institutions in privacy-by-design include IBM and Microsoft Research, Carnegie Mellon University, KU Leuven, CASED and the University of Nijmegen.

The UK has not had a coordinated approach to research in CPS in general, or cybersecurity of CPS in particular. Relevant UK research rarely carries a CPS label, with much of the relevant work being labelled "Internet of Things" or "embedded systems". It is perhaps interesting that the EU funds CPS and IoT under separate headings in H2020.

Research commercialization

The UK can always learn from other entrepreneurial cyber security eco-systems, Israel being a good example. However, many UK universities have fairly mature routes for commercialization of research and the Royal Society could take a lead in reviewing this with an aim of disseminating good practice more widely. It is not clear that any policy changes are required to facilitate commercialization.

Responsible research and innovation

Cyber security is a socio-technical problem and research should be guided by the Ethical Code which was promulgated by the Council for Science and Technology and institutional research ethics guidelines. UKCRC supports the work on a Framework for Responsible Research and Innovation in ICT (FRRIICT) being led by the University of Oxford. Much of the research in British universities has dual-use potential and, within the ethical guidelines discussed above, it should remain a matter of personal conscience as to what extent academics engage in dual-use exploitation of their results.

Public awareness of cybersecurity and, in particular, public understanding of cyber risk should be a priority. At the school level this could be achieved by the creation of appropriate MOOCs. For more mature computer users, there may be a role for cyber insurance. It is probably a Government responsibility to take a lead on this.

Research co-ordination and informing policy

The routes for academic influence on policy are ad hoc. This comment is not specific to cyber security but is more generally applicable to national security. A more systematic approach could result from creating a national academic forum which could engage in a conversation with government and industry on specific challenges – this a logical conclusion of the ambitions expressed in the White Paper on Security Through Technology. There are a number of bodies that might already claim to do this for cyber (BCS and its academy, the IET, the Information Assurance Advisory Council) but their coverage is partial.

UKCRC would be pleased to provide further detail of any of the issues raised above, either in writing or by way of oral evidence. This response was coordinated by Professor Chris Hankin (c.hankin@imperial.ac.uk).