Advancing Cybersecurity Research and Education in Europe

Major Drivers of Growth in the Digital Landscape

Cybersecurity Policy White Paper

Europe Policy Committee
Association for Computing Machinery

October 2016

ACM Europe Policy Committee

Fabrizio Gagliardi (Chair)

Report Authors

Fabrizio Gagliardi (Chair)
Barcelona Supercomputing Center

Chris Hankin
Imperial College London

Judith Gal-Ezer
Open University, Israel

Andrew McGettrick
University of Strathclyde Glasgow

Maarja Meitern
ACM Europe Research Assistant

Report Reviewers

Gerhard Schimpf
Chair, ACM Europe Council of European Chapter Leaders

Hervé Bourlard
Idiap Research Institute

Manel Medina
APWG.eu R&D coordinator, esCERT-UPC

Robert B. Schnabel
ACM Executive Director and CEO

Renee Dopplick
ACM Global Policy Director

https://www.acm.org/public-policy/euacm

Association for Computing Machinery
ACM brings together computing educators, researchers, and professionals to inspire dialogue, share resources, and address the field's challenges. As the world's largest computing society, ACM strengthens the profession's collective voice through strong leadership, promotion of the highest standards, and recognition of technical excellence. ACM supports the professional growth of its members by providing opportunities for life-long learning, career development, and professional networking. ACM's Councils in Europe, India, and China foster networking opportunities that strengthen ties within and across countries and technical communities. Their actions enhance ACM's ability to raise awareness of computing's important technical, educational, and social issues around the world.

ACM Europe Policy Committee
The ACM Europe Policy Committee serves as the focal point for ACM's interaction with the EU and member states' governmental bodies, the computing community, and the public in matters of European public policy related to computing, informatics, and technology. Its membership reflects a diverse community of computing practitioners, scientists, educators, researchers, and other technology professionals from government, business, academia, and the nonprofit sector. The committee's contributions to public policy draw from the deep scientific and technical expertise of the computing community.

Contents

Introduction

- **Enhancing and Strengthening Cybersecurity**
- **Cybersecurity in Europe**
- **Guiding Principles for Policy Approaches**

About This White Paper

Advancing Cybersecurity Research and Education in Europe: Major Drivers of Growth in the Digital Landscape explores the important role of cybersecurity research and education in enhancing cybersecurity. The paper provides an overview of cybersecurity challenges, explores its multifaceted and multidisciplinary nature, and covers some emergent trends generating new privacy and security concerns. The paper discusses approaches to addressing those challenges through strategic investments in cybersecurity research and development, strengthening the education and workforce pipelines, and improving the integration of ethics and professional responsibility throughout the cybersecurity landscape. The paper identifies twelve guiding principles for public policies to advance cybersecurity research, education, and workforce development.

Contributors and reviewers included a high-level experts group of computing professionals, scientists, researchers, educators, and other technology professionals with backgrounds in a range of computing disciplines, cybersecurity education, and computing education. The paper is informed by their expertise, leading reports and publications of ACM members, government reports, and key industry best practices, standards, and resources.

The paper represents the views of the ACM Europe Policy Committee and does not necessarily represent the views of the Association.

Introduction

Governments and industry leaders from every major sector widely recognize the importance of strengthening the cybersecurity landscape. The rate of technological development is producing a rapidly changing set of challenges.

Transformative developments in computing power, cloud computing, mobile, artificial intelligence, ubiquitous interconnectivity, and large-scale automated systems are bringing novel and powerful concerns for cybersecurity, privacy, and safety. The implications for future privacy and security threats are ominous and could have implications for decades to come.

Public trust in the integrity of our global financial systems, information networks, and other critical infrastructure systems is essential for continued economic growth, public safety, and innovation. Maintaining and providing improved, secure, resilient, and trustworthy digital ecosystems is vital to protecting organizational and personal data against a growing range of cyber threats and vulnerabilities.

Achieving strong cyber resilience and cybersecurity leadership in Europe will require coordinated individual and collective action to safeguard and continually strengthen the cybersecurity ecosystem.

The adoption of the first EU-wide cybersecurity legislation on 6 July 2016 marked a significant advancement in fostering crossborder cooperation by

Member States and boosting enhanced security by businesses providing essential services and critical infrastructures. The Directive on security of network and information systems (the NIS Directive) entered into force in August 2016.

The European Commission's Digital Single Market Strategy and the advisory Scientific Advice Mechanism recognize cybersecurity as a core policy priority. The EU Cyber Security Strategy provides a policy framework for EU initiatives.

The ability to address legacy vulnerabilities, weaknesses in current infrastructures, and future threats depends on growing a strong research and development community.

The European Union, through its Horizon 2020 research agenda, has invested €160 million in cybersecurity research and innovation projects. The European Commission also plans to invest an additional €450 million during 2017-2020 in a new public-private partnership on cybersecurity, the Cybersecurity cPPP.

Increased government-funded research and public-private coordination is needed, particularly in the expanding fields of new secure networking and computing architectures, high-performance computing, encryption, data integrity, artificial intelligence, big data, privacy, and risk management strategies.

Governments should provide legal protections for legitimate and beneficial computing privacy and security research.

Satisfying the growing demand for a skilled computing and cybersecurity workforce requires expanding educational opportunities for students at all levels, increasing the number of qualified educators, providing training opportunities throughout employment, and aligning educational pathways with advanced education and careers in computing and cybersecurity. Cybersecurity education and workforce development plans should address diversity and inclusiveness.

Cybersecurity Objectives of the European Commission

- *Increase cybersecurity capabilities and cooperation*
- *Make EU a strong player in cybersecurity*
- *Mainstream cybersecurity in EU policies*

Cyberspace crosses geographic and governance boundaries. Continued efforts are needed to advance and coordinate cybersecurity policies, laws, regulations, guidelines, and best practices. Governments, industry, academia, and organizations play individual and integrated roles in protecting the privacy and security of data, networks, computers, and devices.

Intergovernmental cooperation at the local, national, regional, and international levels can facilitate effective and harmonized legal and policy frameworks.

Outreach efforts are needed to raise awareness among governments, companies, organizations, and individuals about the importance of cybersecurity and technical and ethical best practices to ensuring a strong cyberspace.

12 Guiding Principles for Public Policies to Advance Cybersecurity Research and Education

1. **Cybersecurity Research and Education as Public Policy Priorities**
   Strengthening cybersecurity research, education, and workforce development are vital to achieving overall cybersecurity policy objectives.

2. **Cybersecurity as Multifaceted and Multidisciplinary**
   Research and education policy approaches will be effective only if they encompass the multifaceted and multidisciplinary nature of cybersecurity.

3. **Cybersecurity and Privacy as Complementary**
   Security and privacy are complementary concerns, rather than tradeoffs. Planning should address both aspects.

4. **Build in Security and Privacy**
   Security and privacy should be built in as part of the culture, approaches, processes, systems, and technical infrastructures.

5. **Cybersecurity Research and Development Funding**
   Research and development funding is indispensable to cybersecurity and innovation and needs to address both security and privacy.

6. **Cybersecurity Research Opportunities in Higher Education**
   Expanded opportunities for students and faculty to engage in cutting-edge and high-impact research are important to growing a strong research community.

7. **Legal Protections for Privacy and Security Researchers**
   Governments should provide legal protections for individuals conducting legitimate and beneficial computing privacy and security research.

8. **Cybersecurity Education and Workforce Pipelines**
   Expanded access to cybersecurity and computing education at all levels is needed to prepare, build, and improve the workforce. Policy approaches should address diversity and inclusiveness.

9. **Educator Professional Development**
   Ongoing professional development enables educators to gain and update their knowledge and skills, and supports high-quality instruction to improve student learning.

10. **Public-Private Coordination**
    Improved coordination of the public and private sectors is needed to address cybersecurity research and education.

11. **Public Engagement**
    Cybersecurity public advisory boards, research review boards, and public forums should include representation from the computing field.

12. **International Cooperation**
    International cooperation plays a key role. Cybersecurity challenges and benefits flow across borders and globally interconnected systems.

Cybersecurity Challenges and Approaches

- **Multifaceted, Multidisciplinary Nature of Cybersecurity**
- **Understanding Technical Vulnerabilities**
- **Future Trends and Emergent Technologies**

Cybersecurity Challenges and Approaches

Digital systems are pervasive and cover a large spectrum from personal devices, to large corporate systems, to control systems operating our critical infrastructures.

Government, industry, academia, and organizations play individual and integrated roles in information sharing, prevention, detection, investigation, crisis response and recovery, and risk management strategies to safeguard data, networks, computers, and devices.

Multifaceted and Multidisciplinary Nature of Cybersecurity

Cybersecurity is a multi-faceted and multidisciplinary computing-based discipline involving technology, people, information, and processes to enable assured and trustworthy operations.[1] It involves the creation, operation, analysis, testing, monitoring, and improvements of secure computer systems.

Cybersecurity includes aspects of policy, law, ethics, risk management, and human factors. Legal, regulatory, and policy frameworks need to address security while protecting public safety, ensuring confidentiality and privacy of information, and enabling innovation.

Cybersecurity is an inherently multidisciplinary endeavor requiring policy leaders, computing professionals, researchers, mathematicians, engineers, social scientists, ethicists and psychologists to achieve its objectives.

Why Is Cybersecurity Important?

In its 2015 Cyber Threat Report Symantec Corporation reports that, as a conservative estimate over half a billion personal records were lost or destroyed in 2015, there were over one million cyber attacks against people each day, 75% of all legitimate web sites were vulnerable to attack in such a way as to potentially infect users, a new form of attack was appearing roughly once every week.[2]

The recent Cyber Security Breaches Survey from the UK government reports that two thirds of large UK businesses were hit by a cyber breach or cyber attack in the past year, with one in four being hit by a breach at least once per month. The cost of these attacks often runs into millions of pounds/euros/dollars.

In short, cyber issues pose a serious threat to everyone and to all organisations.

Standing back from the financial and economic arguments, advances in computers and computing technology are shaping the world and society and that brings huge challenges and a huge responsibility. There are many ethical issues involved and being sensitive to these is vital for the development of a fair, just, safe and secure society which at a digital level is being fashioned for future generations.

A secondary aspect of this is ensuring that businesses are secure and that individuals feel safe and comfortable with the use of the technology.

Understanding Technical Vulnerabilities

Cyber vulnerabilities arise in a number of different ways. Cybersecurity covers a spectra of technologies, networks, and related infrastructures and provides protection from intrusion, data theft, and interference with or damage to systems, networks, data, and other cyber and physical infrastructures.

The ITU Study Group in 2008 adopted the following definition of cybersecurity:

"Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: availability, integrity, confidentiality."[3]

Availability is having assets available when needed. Integrity ensures data is protected from accidental or unauthorized modification or deletion. Where required, it can be ensured that the data is what its "packaging" claims it to be (authentication) and that in a two-party transaction, neither party can deny their involvement (non-repudiation). Confidentiality is ensuring information is not made available to unauthorized actors (people, entities or processes).

In combating threats, a number of observations should be made. The area is complex, in a state of constant change and becoming ever more sophisticated.

Risk assessment methods can be used to evaluate risk against the value of the assets to be protected, and to gauge the (proportionate) level of protection required; both quantitative and qualitative approaches can be utilized. Standards such as ISO 27001, and voluntary frameworks, such as the US NIST Cybersecurity Framework, and the SANS Critical Controls are relevant in this regard.

Methods employed in computer security include: the use of (effective) passwords, two factor authentication, biometrics, permissions associated with file access, encrypting of information, the use of mathematical models of information flow, firewalls, intrusion detection, penetration testing and (controlled) offensive activities;

Best practice in software and systems engineering including design principles for secure systems (least privilege, fail-safe defaults, separation of privilege, complete mediation, least common mechanisms, open design) should be used.

The use of multiple diverse methods can be employed using fault tolerant and resilience approaches which ensure that, although one defense may be compromised, the others will maintain overall security; when compromise takes place that defense should then be strengthened or replaced in a timely fashion.

Critical information (e.g. passwords) may be divulged inadvertently or by taking inadequate precautions; problems can arise with poor software practices including using software that has not been properly tested; viruses or other malware (malicious software) can travel between computers; spyware seeks to extract information about users by devious means; communications may be intercepted; overloaded sites can generate problems. The possible existence of 'insider threats', i.e. threats from people such as employees or consultants must be recognised.

Cyber breaches can result in all aspects of computer operation being compromised. This includes bringing down or interfering with, e.g. defacing, web sites (resulting in loss of business or general chaos), compromising critical infrastructure, reductions in safety and security in certain applications (e.g. cars or transport, health) loss of privacy to individuals (e.g. with banking details being accessed), loss of service, changes to information, and so on. In considering these issues, it is important to recognize that: computers can be used to attack other computers resulting in many rapid attempts at finding vulnerabilities; computers themselves are becoming ever more sophisticated and exhibiting aspects of intelligence; with developments involving the internet-of-things many small devices will be connected to the internet and there is the possibility that many of these will exhibit lower quality security than larger systems.

Future Trends and Emergent Technologies

- ***Internet of Things***

The Internet of Things (IoT) incorporates a wide variety and significantly increased number of interconnected devices, sensors and infrastructures. The growing IoT landscape is across differing technical systems, networks, protocols, and standards, and spans into control of objects in the physical world. The pervasiveness, decentralized nature, and variety of interactions create new complexities and implications for safety, security, privacy, reliability, and resilience.

Some of the vulnerabilities in Internet of Things products have had exposure by attacks on high-end automotive systems.[4] The objective of cyberattacks on these systems is often sabotage rather than stealing data. The links between cybersecurity and the physical effects is often quite subtle. The systems are often managed by control engineers who have other concerns than cybersecurity and cybersecurity solutions are often inappropriate, particularly in safety critical systems. For example, one of the most effective controls in traditional cybersecurity is aggressive patch (vendor software updates) management, whereas in some cyber physical systems patches are never deployed because their deployment destroys any safety case.

- ***Cyber Physical Systems***

A relatively recent phenomenon, which will accelerate with the roll-out of the Internet of Things, is the interaction between digital systems and the physical world. One of the earliest indications of the cybersecurity challenges that this might pose was the identification of Stuxnet in 2010.[5] Since then there have been a number of high profile attacks on industrial control systems including the destruction of a German steel

mill blast furnace in 2014 and the Ukrainian power outages in 2015.

Cybersecurity Research

- **Enhancing the Research Pipeline**
- **Coordination of Public and Private Sectors**
- **Priority Cybersecurity Research Areas**

Cybersecurity Research and Development

Dedicated public and private funding for cybersecurity research and development is indispensable to Europe's cybersecurity and innovation. Investments are needed to expand the speed and scale of research and development.

Security and privacy are complementary concerns, rather than tradeoffs. Research priorities should address both aspects.

Enhancing the Research Pipeline

Because of the ever-evolving nature of the cyber world and its importance, funding is needed to support top-class fundamental and applied research and the pipeline of researchers within the public sector, academia, and industry.

Cybersecurity research should cover a broad spectrum from challenge-led long-term research through to more applied research which can lead to immediate improvements in practice. An example of the former is the DARPA Grand Challenge in Cybersecurity which called for automatic defensive systems which could reason about flaws, formulate patches and deploy them in real-time. An example of the latter is work from the UK's Research Institute in Science of Cybersecurity which has informed new password advice from the UK Government.

Cybersecurity research calls for a diverse range of skills from engineering, mathematics, computer science and human sciences such as psychology.

Public-Private Coordination

Coordination of public and private investments in research and development will help spur the necessary scope and scale of research vital to developing next generation cybersecurity technologies, ecosystems, tools, solutions, and processes. To be successful a close partnership across government, academia, and industry is essential.

Cybersecurity public advisory boards for research agendas and research review boards should include representation from the computing field.

Priority Cybersecurity Research Areas

The rate of technological development is producing a rapidly changing set of challenges. The following are a few priority areas where further and new research could encourage the development of more secure digital ecosystems and inspire innovation.

- ***Developing a Science of Cybersecurity***

As Fred Schneider has observed, a science of cybersecurity should provide a body of knowledge that enables the prediction of the outcome of design and implementation choices.[6] Many scientific disciplines include some notion of measurement. However, the lack of constraints on the behaviours of both attackers and defenders make good cybersecurity metrics quite elusive.

A first step could be to establish research protocols to ensure that experiments are reproducible.[7]

A science of cybersecurity might ultimately enable the quantification of improvements in security achieved by certain measures and also generally support better risk-based decision making.

- ***Verification and Validation***

Society's increasing reliance on digital technologies which are driven by software, often provided as binary code by third party suppliers, raises the importance of being able to verify, or at least validate, the security of systems. There have been some impressive results already in using program analysis and bounded model checking tools. Despite these promising developments, generic solutions which operate at appropriate industrial scale remain a significant challenge. Progress in this area depends also on the vision of the DARPA Cyber Grand Challenge mentioned earlier.

- ***Cyber Physical Systems***

Cyber-physical systems integrate computing, networking, and physical components and processes. There are a number of challenging privacy, security, and public safety research problems to be addressed in this area, including the use of algorithms and feedback loops where the physical processes impact the computations, with substantial programmes in the EU (both H2020 and national programmes) and the US.

- ***Secure Hardware***

Traditionally, much of the cybersecurity technology has been in the form of software. Increasingly mechanisms are being implemented in hardware. Typical candidates for hardware implementation are controls which involve network monitoring such as hardware firewalls and hardware security modules employed in tamper-proof cryptography. Some authors have suggested that the deployment of Internet of Things may lead to a greater need for hardware security technologies.[8] Some of the research challenges include developing a better understanding of the scope and limitations of hardware security technologies and identifying and understanding barriers to exploitation.

- ***Network Security***

Software Defined Networks (SDN) are currently attracting a lot of attention. The key idea is that high-level flow routing decisions are made at control layer, which is software controlled and decoupled from the lower level data handling layer. Many of the early approaches to SDN were based on the OpenFlow protocol. The decoupling of high-level routing decisions from data handling raises the possibility of innovative approaches to network security as exemplified in the Fresco system.[9]

The concept of Total Network Defence is also attracting some attention as a research challenge. This involves developing new ways to detect, classify and defend an entire network against malicious software, by combining data from several sources such as: network captures; firewall activity; virtual machine images; host-based sensors; etc.

- ***New Computing and Network Architectures***

If we do not succeed to build more trustworthy components and systems,

sooner or later we will run into a cybersecurity crisis on a national or international level. Given the rising number of successful attacks (e.g. the German Bundestag) and breaches it is clear that the current arsenal of security measures are not effective enough. The current IT architectures are too complex and the increased complexity translates into growing numbers of attack vectors. The present defense strategies build on what we understand and do not entirely address the fundamental weakness in system architecture design and implementation.

- ***Security and Privacy by Design***

Security and privacy must be built in from the outset, very much like engineers address safety when they build airplanes or other safety-critical systems. These new-type systems must be deployed when it comes to critical infrastructures, such as the electric grid, manufacturing facilities, transportation vehicles, financial institutions, water treatment facilities and water supply, food supply, and weapon systems. Research is needed on improved ways to approach security and privacy by design and effective instructional pedagogical practices in this area.

- ***Cryptography***

Cryptography is a very active area of research, particularly concerning proofs of the computational complexity of cryptographic systems. Two more recent areas that are receiving increasing attention are: Homomorphic Encryption and Quantum resistant cryptography.

The ability to process encrypted data without the need to decrypt it first promises huge gains in security and privacy. The cryptographic approaches which support this capability are collectively known as Homomorphic Encryption.[10] Whilst there has been a substantial amount of work in this area, performance issues remain a significant barrier to widespread adoption.

Public and private investment in cybersecurity research and development is indispensable to Europe's cybersecurity, competitiveness, and innovation.

Many traditional approaches to cryptography rely on the computation intractability of factoring large numbers or other hard problems in number theory such as solving the elliptic curve discrete logarithm problem. Should Quantum Computing become a practical proposition, Shor's integer factorisation algorithm[11] would break these approaches. There is hence a challenge to develop quantum resistant approaches to cryptography; the key is to find intractable problems which are not amenable to fast quantum computer-based solutions. Lattice-based approaches to cryptography are one promising avenue of work and also may provide an approach to Homomorphic Encryption too.[12]

- ***Identity Management***

Since a White House report in 2011, there has been substantial interest in the creation of an Identity ecosystem which would help

with the creation of privacy-enhancing trusted digital identities.[13] This seems to be a prerequisite for the establishment of a truly digital society; the alternative seems to be the status quo where authentication is done on an ad hoc basis with all citizens having to cope with the cognitive load of multiple strong passwords. Central to this notion of an identity ecosystem is the development of anonymous credentials.[14] Work on this has concentrated on the development of next generation biometrics. There has been quite a lot of work done on anonymous identification of fingerprints – this is achieved by the selection of a small number of features which are sufficient to authenticate for the purpose at hand. Questions remain as to whether such approaches are scalable and commercially viable. This is likely to be a very active area of research for the foreseeable future.

- ***Human and Social Sciences***

Many of the most significant security failures involve humans and can often be attributed to poor design that fails to take the human factor into account. The earlier cited guidance on password choice is an excellent example of an attempt to rectify this situation. Few security solutions are likely to succeed without involvement of human factors specialists. Cybersecurity is a truly multi-disciplinary endeavour and much more research is needed on the human dimensions of cybersecurity. This work requires input from psychologists and the social sciences as well as computer scientists, mathematicians and engineers.

- ***Ethics in Research***

We need to bear in mind that working with malware is not ethically neutral. One needs to "think like the criminal who wrote it in the first place."[15] Therefore, the professionals and students working with these topics should be trained to "think nefariously so that it does not overtake their ability to reason morally."[16]

In addition, to these concerns malware research might affect the real lives of people, as the researchers might have access to private compromised machines while studying malware in situ. Thus, there is also a need to prepare the cybersecurity community to those novel and often unexpected situations which are not related to the subjects of their initial research. Cybersecurity researchers are facing without a doubt novel ethical challenges "that exert a strong influence on online trust."[17]

Cybersecurity Education and Workforce

- **Computing and Cybersecurity Education at All Levels**
- **Cybersecurity Workforce Development**

Cybersecurity Education and Workforce Development

Providing inclusive access to computing and cybersecurity education at all levels and strengthening workforce development are vital to achieving cybersecurity policy objectives. Local, state, national, and regional education and workforce development plans should align policy, programs, and resources to support growth in cybersecurity education and jobs.

Pre-University Cybersecurity Education

There are many different approaches to the teaching of computing at the pre-university school level (primary and secondary). If, in addition, computing is taught in such a way that the use of computers by pupils is safe, secure, and responsible and yet disciplined, useful and stimulating, then cybersecurity concerns will be addressed.

Teachers are the key to the success of any study program, thus it is expected that teachers teaching cybersecurity have formal education and are well trained on the subject. However, many teachers of computing do not possess a first degree in computer science or they have graduated in computing some years ago. The teaching of issues related to cybersecurity is nontrivial and changing with time. The dynamic and evolving nature of computing and cybersecurity require ongoing training of teachers. Appropriate formal education for teachers with relevant in-service or pre-service education is desirable.

Higher Education

The computing curriculum in higher education needs to address cybersecurity concerns to ensure that graduates: (a) enter the workplace with a strong ethical code and capable of developing systems without cybersecurity vulnerabilities, (b) are well placed to help combat cybersecurity threats, and (c) understand that security is a complete systems issue.

ACM produces and keeps current international curricula recommendations and guidelines in all areas of computing, including cybersecurity.[18] These guidelines are used in the United States and worldwide to standardize and assist in the accreditation of college and university programs.

ACM's Cybersecurity Curricula Recommendations and Guidelines are used around the world.

The ACM Joint Task Force on Cybersecurity Education, launched in September 2015, currently is developing comprehensive international curricular guidance in cybersecurity education to support future educational efforts.[19] The Joint Task Force is a collaboration between major international computing societies: ACM, the IEEE Computer Society (IEEE CS), the Association for Information Systems Special Interest Group on Security (AIS SIGSEC), and the International Federation for Information Processing Working Group on Information Security Education (IFIP WG 11.8). The Joint Task Force grew out of the foundational efforts of

the Cyber Education Project.[20]

The implications of these observations have a profound impact on all phases of the computing curriculum, perhaps most obviously in programming, software development, the human computer interface, communications, databases, operating systems, concurrency, security, information management, professional ethics, systems engineering and even in hardware courses. Both theoretical and practical or hands-on aspects, and the important link between these, need to be addressed.

These considerations provoke the question: should cybersecurity be offered as an autonomous discipline at undergraduate level? Thinking on this is divided and changing, but generally it seems too early to give cybersecurity this status; but a variety of authoritative courses in cybersecurity at Masters level is desirable, with prerequisites being a sound background in disciplines such as computer science, software engineering, business computing, etc. For students in disciplines other than computing, often a general course on computational thinking is offered and these can address cybersecurity considerations. More generally cybersecurity issues can be integrated into general study programmes to prepare attendees to use computers and the Internet intelligently, safely and securely.

The rate of change and the increasingly sophisticated threats are on-going issues for educators and researchers at colleges and universities. Ongoing professional development enables educators to gain and update their knowledge and skills, and supports high-quality instruction to improve student learning.

Expanding research opportunities for students and faculty to engage in cutting-edge and high-impact research is important to growing a strong research community.

Cybersecurity Workforce Development

Given the rate of developments in cybersecurity, there is an ever pressing need to keep software professionals up-to-date with developments in cybersecurity. Senior managers need to be keep abreast of the latest best advice. In all these cases, educational issues are ever present.

Professional bodies, professional societies or support groups are typically well placed to offer access to appropriate education, even issuing certificates to ensure currency.

Cybersecurity Ethics

- **Cybersecurity Ethics in Modern Society**
- **Public Awareness Campaigns**

Cybersecurity Ethics

With the accelerating convergence of the physical world and the cyber world, computing ethics is now becoming a general concern for all stakeholders including end-users, service providers and authorities.

Autonomous driven cars, robots performing surgical operations, social networks, etc., all are manifestations of the new cyber world which requires a responsible and ethical approach from everybody involved and not just from the system developers.

Cybersecurity Ethics in Modern Society

In all cases, public outreach and education need to be imbued with ethical and legal considerations that serve to guide the development of a society that is in tune with the best principles of safety, security, fairness and justice.

- ***ACM Code of Ethics and Professional Conduct***

The ACM Code of Ethics and Professional Conduct, adopted on 1992 and currently going through a review process, covers well the ethical responsibilities of computer professionals and academics.

Two principles from the ACM Code of Ethics are especially important for cybersecurity: first, principle 1.2 *"avoid harm to others*" and second, principle 1.7 *"respect the privacy of others*". Computer professionals are requested by code of ethics to operate taking into account the potential harm that lack of ethical standards might cause. However, the specific role of cybersecurity professionals might be very different from one to another. For this reason a code of ethics,[21] although a good start, might not always be sufficient and should be enforce also by educational means. In addition, like in other professions where ethics plays an important role, such as journalism, there is the dilemma whether a breach of the ethical code should be sanctioned. Although so far this has not been the case, the ACM Code of Ethics has played a role in court proceedings in the US (e.g. *Oracle v. Google*).[22]

Nonetheless, until these dilemmas are solved one thing is for sure - education and training can help the professionals to further understand the wider impact of their work when dealing with ethical issues.[23]

- ***Critical Infrastructure Ethics***

National Governments have the responsibility to promote the implementation of cybersecurity mechanisms in public administrations and private sectors, through legislation, regulations, and also economic incentives. They have also responsibility to take care of citizens' and enterprises' cybersecurity, reinforcing the skills and capabilities of Law Enforcement Authorities, and creating adequate supervisory agencies. Some research is being made to support those decision makers, to evaluate the impact of cybersecurity strategies at national level, e.g. APWG, STC, CyberGreen.

Critical Infrastructure operators must perform risk analysis of their infrastructures, in order to demonstrate the adequacy of the

cybersecurity measures set in place to protect the infrastructure. They should be aware that the issues analysed in the risk management process, should include the potential damages caused to the Society by discontinuity or irregularities in the provision of the critical services, even if those have small direct economic cost in the critical infrastructures themselves. The research being made in this area addressed two focuses: a) real time vulnerability and impact analysis; b) intelligence analysis of environmental and situational scenarios.

- ***Developers' responsibility***

Cyber systems developers have the prime responsibility to develop safe systems based on sound ethical principles. In general, we expect developers to produce high quality software with high safety standards. If economic or personal interest lead to badly written code or even worse malicious code, severe consequences to others may result. For example, the case of Volkswagen's "defeat device", where the programmed software algorithm enabled the cars to cheat the emission tests.[24]

Computers in their pervasive and powerful presence are allowing new possibilities to harm others which are often difficult to detect. Developers have therefore, the responsibility to make sure that what they produce will not cause harm to others and are in accordance with the fundamental society's ethical principles.

- ***Ethics in education***

For the abovementioned reasons, ethics should be a mandatory part of computer science education. Therefore, it is important to educate students and to involve institutional ethical committees in education systems. Preparing students for dealing with ethical dilemmas prior to graduation would prepare them at least for some possible ethical dilemmas they might face. There are many ways how to approach ethics in the computer science curricula, for example if the subject is dealing with building secure systems the material on these aspects has a value for the community and should be shared as good practice. Another example is when certain forms of attack are taught, as it is also important to show the students the appropriate restrictions. Just as medical researchers study viruses in safe environment it might be necessary and useful to teach how to build viruses and worms to cybersecurity students. Students need to understand the working of these mechanisms if they were to combat them, but at the same time it will be necessary to explain the consequences and the ethical issues that their actions can cause in real people lives and not just in the virtual world.[25]

- ***General public and ethics***

It is not just the professionals who bear the burden to act ethically when developing programs, the end-users as well have an ethical responsibility. It is important to raise public awareness of the dangers and assist in ensuring that computer use by the general public is safe and secure as well as being interesting and rewarding. For example, people should care about protecting their own data, either as an individual or as a company. Different datasets may contain information that could harm others and not only the end-user itself. For example, it is widely recognized that cloud computing's expectations of trustworthiness may be unrealistic.[26]

Therefore, companies should evaluate what kind of information is ethically responsible to share through cloud. Although at the end each individual has to decide on the legitimacy of his\her actions, we need to be aware that in order to live in a safer connected world everybody need to make a morally correct decisions and help others to understand the importance of ethics in the cyber environment.[27]

Public Awareness Campaigns

Within the general public there ought to exist a culture of cybersecurity awareness. This includes, for example, realizing that identity theft and / or financial loss can be the consequences of attacks. To guard against these, computers and data have to be protected. The means of access, e.g. passwords, have to be thoroughly secure and not shared with other parties. Up-to-date anti-viral software has to be installed and system software has to be kept current since updates are often provided to address security breaches.

The duty of parents / guardians or folk in positions of responsibility, includes being alert to the pitfalls of uncontrolled access and be able to take positive steps to ensure safety, security and positive interaction by their clients with computer systems. In order to be able to fulfil their duty, they have to acquire the relevant knowledge or take appropriate steps and this includes being ever vigilant to change.

Analogy to Public Health Awareness Campaigns

Public health and cybersecurity can be viewed as involving 'infection control', one in the real world, the other in the digital world. In both cases threats exist and need to be assessed. These threats can spread and become widespread, they mutate and change, and they need to be closely controlled. In cybersecurity just as in the area of public health, authorities need to be alert and prepared to fight the threats that can spread, mutate and change, in order to prevent harm to the public.

Public health is relatively mature as an area of endeavor. But authorities will typically embark on a range of activities such as: for a virus such as norovirus, explaining what the symptoms are, how it spreads, how to reduce its impact; publishing weekly reports on an outbreak of, say norovirus; providing control measures when there is an influenza outbreak, say; providing general infection prevention and control precautions not just for viruses but for other harmful organisms. In addition, they will investigate the causes of infection (and act on the results), they will carry out audits on institutions (or parts thereof), and they will educate staff.
In addition to the above, public health authorities ensure that steps are taken to inoculate and to guard against serious illness and they will provide health advice and services to the public, e.g. through immunization, so reflecting a community role. Generally, all these public health activities are publicly financed.

Conclusions

We hope with the present paper to have contributed to the current ongoing discussion in Europe on a subject like cybersecurity, which is becoming of vital importance for the implementation of the digital European strategy. The ACM policy committee in Europe will continue researching on this subject and will remain available to consult with the European Union authorities in Brussels and in the member states.

Acknowledgements

We are grateful for the review and input from our colleagues in the ACM U.S. Public Policy Council and Renee Dopplick, ACM Global Policy Director. They suggested a number of subjects for future work, which will be pursued further.

References

[1] ACM Joint Task Force on Cybersecurity Education, http://www.csec2017.org.
[2] Symantec, http://www.symantec.com.
[3] ITU, http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx.
[4] A cyber attack on a Jeep can be viewed at https://www.youtube.com/watch?v=MK0SrxBC1xs (accessed on 17th August 2016).
[5] Langner, R (2016) *To kill a centrifuge* accessed at http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf on 17th August 2016.
[6] Schneider, F. (2012) *Blueprint for a Science of Cybersecurity*, The Next Wave, 19(2), 47—57.
[7] http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-039.pdf accessed on 15th August 2016.
[8] Lesjak, C. et al (2015) *Hardware-security technologies for industrial IoT: TrustZone and security controller*, IECON 2015, IEEE Press.
[9] Shin, S. et al (2013) FRESCO: *Modular Composable Security Services for Software-Defined Networks*, ISOC Network and Distributed Systems Security Symposium.
[10] Gentry, C. (2009) *A Fully Homomorphic Encryption Scheme*, Stanford University PhD dissertation, September. Available at https://crypto.stanford.edu/craig/craig-thesis.pdf.
[11] Shor, P. (1999) *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,* SIAM Rev 41(2).
[12] D. Micciancio and O. Regev: *Lattice based Cryptography,* accessed at https://www.cims.nyu.edu/~regev/papers/pqc.pdf.
[13] http://www.idesg.org/About/Overview.
[14] http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8054.pdf.
[15] Sullins, J.P (2014) *A Case Study in Malware Research Ethics Education When teaching bad is good*, IEEE Security and Privacy Workshops, Retrieved 18/08/2016 at: http://www.ieee-security.org/TC/SPW2014/papers/5103a001.PDF.
[16] Sullins, 2014, p.2.
[17] Kenneally, E. & Bailey, M. (2014) *Cyber-security Research Ethics Dialogue & Strategy Workshop*, ACM SIGCOMM Computer Communication Review, volume 44, number 2, April. Retrieved 08/22/2016 at: https://www.caida.org/publications/papers/2014/creds2013_report/creds2013_report.pdf.
[18] ACM Curricula Recommendations and Guidelines, http://www.acm.org/education/curricula-recommendations.
[19] ACM Joint Task Force on Cybersecurity Education, http://www.csec2017.org.
[20] Cyber Education Project, http://www.cybereducationproject.org.
[21] http://web.cs.wpi.edu/~hofri/Readings/ImpactAcmCode.pdf accessed on 19th August 2016.
[22] http://ethics.acm.org/code-of-ethics/using-the-code/ accessed on 22nd August 2016.
[23] Brey, P (2007) *Ethical Aspects of Information Security and Privacy,* Security, Privacy and Trust in Modern Data Management, M.Petkovic & W. Jonker (eds.).
[24] http://www.theregister.co.uk/2015/09/19/volkswagen_pollution_cheat_claims_epa/ accessed on 20th August 2016.
[25] http://cacm.acm.org/magazines/2005/1/6327-not-teaching-viruses-and-worms-is-harmful/fulltext accessed on 19th August 2016.
[26] http://cacm.acm.org/magazines/2014/10/178776-risks-and-myths-of-cloud-computing-and-cloud-storage/fulltext accessed on 19th August 2016.
[27] Peslak, A. R. (2007). A Review of the Impact of ACM Code of Conduct on Information Technology Moral Judgement. Journal of Computer Information Systems. Retrieved 3/27/2014 at: http://web.cs.wpi.edu/~hofri/Readings/ImpactAcmCode.pdf.