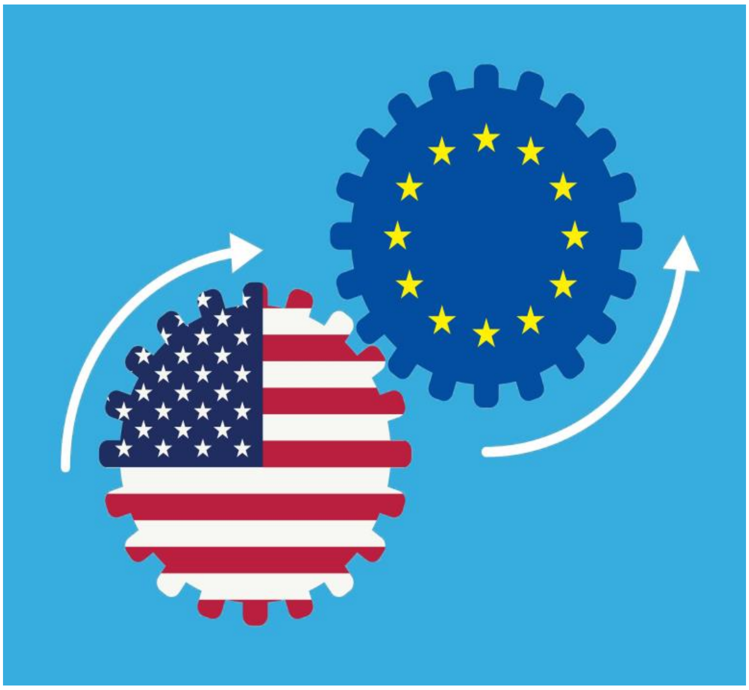
JRC TECHNICAL REPORT

Influence of Research on the Competitiveness of the Security Industry– An EU-US comparison



Naouma KOURTI
Joint Research Centre

Bert COURSEY
National Institute for Standards and Technology

2015

EUR 27403 EN

Influence of Research on the Competitiveness of the Security Industry– An EU-US comparison

This publication is a Technical report by the Joint Research Centre, the European Commission's in-house science service. It aims to provide evidence-based scientific support to the European policy-making process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use which might be made of this publication.

Contact information
Naouma KOURTI
Joint Research Centre, Via Fermi 2749 21027 Ispra Italy
E-mail: naouma.kourti@ec.europa.eu
Tel.: +39 0332 786045

JRC Science Hub
https://ec.europa.eu/jrc

JRC96958

EUR 27403 EN

ISBN 978-92-79-50547-8

ISSN 1831-9424

Doi:10.2788/082867

Abstract

The study on the “influence of research on the competitiveness of the security industry in EU and the US” was carried out during a EU fellowship in Washington, DC’s George Mason University. The fellow has shared her time between the George Mason University and the National Institute of Standards and Technology (NIST). This study was prepared in collaboration with NIST. The analysis has shown that research can influence the security industry by enhancing collaboration, by improving availability of experimental capabilities and by accelerating standardisation.

Executive Summary

The study has three parts. The first discusses the EU and US research programs in general and tries to draw similarities and differences. The second looks in more detail at the security research programs and again tries to draw similarities and differences as well as make some recommendations for improvement. The third part looks into CBRN (chemical, biological, radiological and nuclear) research. It is also divided in three parts: General aims of CBRN research in the EU and the US, the procurement process as a driver for development and innovation, and a current look at standards.

The main conclusions are:

- The EU's research program is managed centrally, it is fully competitive and mostly collaborative (consortia with 3 partners and more) with all partners being contractually committed. Full visibility to all projects is granted through public websites and databases. The US research (non-defense) is managed by each department separately, great amounts of the research budget cover the expenses of the various national labs. Almost all departments have such labs. The rest of the budget goes to grants and project contracts. Evaluation mechanisms are not fully transparent for all departments. Collaboration with other stakeholders is increasingly required but contracts are often awarded to a single entity. Deliverables from projects and grants are not always given sufficient visibility by the departments.
- The main bulk of basic research in the US is managed by DOD for defense, NIH for medical and NSF for all other disciplines. However, all departments may award grants or contracts for basic research. In Europe it is managed by European Research Council (ERC). The US National Science Foundation (NSF), the US National Institutes of Health (NIH) and the EU ERC use evaluation by external experts and maintain public databases of funded projects and their achievements. There is limited exchange between the EU and the US Institutions in basic research.
- US National labs are instrumental for the advancement of science and the development of technologies and methodologies. In the EU experimental work is promoted by the European Research Infrastructure (ERIC) mechanism, which however remains limited to only a few subjects. In some fields such as security there is little overview of Europe's experimental capabilities. Experimental capabilities are crucial for the testing and evaluation of ideas, technologies and in the end products.
- Security research is structured very similar in both EU and US. However, the US research for homeland security benefits also from the huge defense research budget, since developments there spill over to homeland security applications. Defense research is closely coupled with procurement minimizing the risk to the defense industry. This mechanism is adopted also by DHS for applications such as aviation security (Transportation Security Administration). The EU lacks a procurement mechanism coupled with research development.
- DHS has leveraged the capabilities of NIST to boost standardization in security. NIST's testing and metrology labs have developed testing protocols and recommendations for technology use that have been instrumental to the standardization process. EU's projects may develop such protocols and

recommendations, but such efforts are currently scattered and usually lost after the end of the project. DG HOME's ERNCIP project aims at developing security pre-norms, but the project's small budget allows it to cover only a small fraction of the needed work.

- Utilities in both EU and US have been slow to absorb new security technologies. In many cases they are not aware of state-of-the-art technology, they lack trained security personnel, and agreed-upon procedures for working with authorities to resolve CBRN equipment alarms.
- CBRN technology development in the US is fully under the research-procurement mechanism. Huge amounts of money have gone to the pharmaceutical industry to develop vaccines and antitoxins for the national vaccine stockpile. However, progress has been slow and disappointing. There is hardly any activity of this type at EU level. Development of biological detectors has been slow and decontamination capabilities are disappointing. Innovation has been lagging behind. A reason could be DOD's procurement model adopted also for the vaccines - and most CBRNE technologies - does not motivate the industry to take higher risk in what could be game-changing technology solutions.
- Standardisation plays a major role in industrial competitiveness. The presence of NIST in the US, and a more flexible US standardization process, have supported the development of security standards and some testing and evaluation procedures for security technologies (http://www.nist.gov/national-security-standards/tops.cfm). In Europe this is not happening.

Recommendations are:

The US would benefit from more collaborative research in which small business, academia and organisations are involved with the same contractual obligations as big business in the form of a consortium. Moreover, transparency in the way departments spend their research budgets would contribute towards policies that are more widely accepted and shared.

The EU would benefit from a coupling of research and public procurement for security technologies. Such technologies could be followed from the idea to the production and installation, through a transparent and peer-reviewed process.

Readily accessible experimental capabilities are key to technological development. This must include standards and testing and evaluation (T&E) protocols. The EU has to step up its experimental capabilities, create better networks of laboratories and more funding to develop EU wide test and evaluation procedures for security technologies.

The standardization process in the EU has to be accelerated and complemented with pre-norms, guidelines and recommendations based on industry needs and expert advice. A great amount of consensus documents are produced throughout EU's research projects and they mostly disappear after the projects' conclusions. The EU's single market would benefit from a structured repository of pre-norms, guidelines and recommendations for industry and their customers both in the public and private sectors.

The European Commission’s Joint Research Centre (JRC) could be in charge of establishing the framework, the rules, and the quality control of such a repository for the EU.

Table of Contents

Abbreviation List

AAAS	American Association for the Advancement of Science
ANSI	American National Standards Institute
ASTM	American Society for Testing and Materials
BARDA	Biomedical Advanced Research and Development Authority
CBRN	Chemical Biological Radiological and Nuclear
CBRNE	Chemical Biological Radiological Nuclear and Explosive
CEN/CENELEC	European Standardisation Organisation
CIPS	Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Program
DARPA	Defense Advanced Research Programs Agency
DG RTD	Directorate General Research Technology & Development
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
EPA	Environmental Protection Agency
ERC	European Research Council
ERNCIP	European Reference Network for Critical Infrastructure Protection
EU	European Union
FEMA	Federal Emergency Management Agency
FP	Framework Program for Research
HHS	Department for Health and Human Services
ISO	International Standardisation Organisation
IEC	International Electrochemical Committee
JRC	Joint Research Centre
NIH	National Institute of Health
NIST	National Institute of Standards and Technology
NSF	National Science Foundation
SBIR	Small Business Innovation Research
SME	Small Medium Enterprises
TSA	Transportation Security Agency
US	United States

Introduction

This report is the result of an analysis carried out throughout an EU fellowship in Washington DC and in close collaboration with NIST (National Institute for Standards and Technology). The scope of the study is to analyse the security research programs in both EU and US with the aim to understand how each promotes the competitiveness of the security industry. Sharing of good practices and recommendations for future improvements are the intended outcomes of the study.

The area of freedom, security and justice is of special concern in the EU. However, in this sector the EU has shared competence with the Member States (Treaty of functioning of the European Union article 4). The ever-growing pressure on the policy makers to protect the citizens from any kind of adversity being natural, accidental or intended, such as terrorism, is dictating a concerted approach to the subject. However, interests are strong and the maturity and will to act diverge strongly from Member State to Member State making any common political approach from difficult to impossible. This political dissonance has long-reaching repercussions. There is a lack of uniformity in the degree of protection and crisis management competencies around the EU, which creates a sense of insecurity and mistrust among the citizens. Another problem is the lack of a common EU market for the security industry to direct their products and solutions. As a result this EU industry sector remains atrophic, pray to industries from other countries, and oriented towards non-EU markets, notably the US, in order to be stimulated and become innovative. The security research program was established with the 5th Framework program and has been growing since then. Its main focus is to bring EU's researchers active in the field of security closer, enable dialogue and stimulate common research. More and more it concentrates its efforts in the development of new products, solutions and methodologies. However, it is not clear if that translates into market strength, given the lack of market demand at the EU level.

On the other hand, in the US there were already commercial technologies for security applications that date back to the 1990's and earlier in select areas such as biometrics products, computer security, communications technologies, and protective equipment for fire fighters and law enforcement officers. There were, however, very few performance standards for detectors for weapons of mass destruction, for examples standards for chemical, biological, radiological/nuclear and explosives (CBRNE). The US industry in this sector often worked directly with the US Department of Defense (DOD) to develop equipment to meet military requirements. Following the events of September 2001, the terrorists' attacks in New York and the anthrax letters mailed from New Jersey, there was a large, concerted effort by the US government and US industry to develop products and services to mitigate terrorists' threats. The terrorists' threats continue, but in the last decade the US has faced additional threats from natural disasters (two major hurricanes) and the emerging cyber threat to critical infrastructure and institutions. These have accelerated US federal investments and industry efforts. An additional factor of major importance is the rise of multinational security firms that often split their manufacturing sites between the US and EU. In the US, we may see "green" instruments designed for military applications on the shelf with "yellow" versions for non-military applications. And, these instruments may display results in one set of units for the EU market and yet another for the US market.

In the following chapters we shall see the research programs in detail and will try to come up with useful recommendations for future action.

EU Research Programme

EU Research consists of the Research Framework Programs of the European Union and the Research Programs of the 28 Member States. 2014 was the last year of the 7th Framework Program and the beginning of Horizon 2020. In the past, some of the EU's Directorates General (DGs) maintained their own research budgets, but that has been completely abolished in Horizon 2020.

The Framework Programmes

The budget share of framework programmes to EU's total budget in Table 1 shows a steady increase of the importance of research and innovation in the EU. Security research was a separate title only in the 7th framework program, whilst it was part of the Policy support title in the 6th framework programme. EU's framework programs are managed centrally by the European Commission's DG RTD (Research and Innovation Directorate General) according to rules laid down by regulation (EU) No 1291/2013. Other DGs such as CONNECT for the ICT part, ENER for the energy part, ENTR for space and security, etc. are also involved in the management. Similarly, the evaluation of the proposals is carried out by independent experts according to rules laid down in regulation.

	FP5 (1998-2002)	FP6 (2003-2007)	FP7 (2007-2013)	Horizon 2020 (2014-2020)
Budget	€ 14.96 billion	€ 17.5 billion	€ 53.2 billion	€ 80 billion
% EU budget	~4	~3.9	~6	~8%
Security		Under policy support line	1 400 million	1 700 million

Projects have to have partnerships of at least 3 partners from 3 different Member States. Usually projects have to show a fairly good and relevant partnership across Europe in order to be approved. Partners all receive a separate contract from the Commission and, therefore, are treated equally, and all have a say in the project's decision making. International collaboration is a plus. Often collaboration is requested not only among scientists from various countries but also vertically, i.e., from various stakeholder groups from multiple EU Member States. Overall, most applicants in FP7 come from academia. Second largest come from the various European research organisations, and only one third are from the private sector including SMEs (Small Medium Enterprises) [Sixth FP7 Monitoring Report]. However, in specific sectors such as Energy and Security, private sector and mostly industry are the biggest participants and beneficiaries of the program ranging on average of 60% of the participation rate and half of the budget available for that field. In fields like the environment, industry's participation rate falls as low as 19%. [source: Ex-post evaluation FP7 "Environment", DG RTD 2014]. Industry receives only up to 50% community contribution, whilst SMEs up to 75%.

The research topics and calls for expression of interest can be found in: http://ec.europa.eu/programmes/horizon2020/ . EU's research does not include defense research. In general Horizon 2020 has three big titles for funds distribution:

Societal Challenges	Excellent Science	Industrial Leadership	Other	Total
29.7 billion	24.4 billion	17 billion	7.5 billion	78.6 billion

Within societal challenges the funding goes to Health (7.5 billion), Intelligent Transport (6.3 billion), Energy (5.9 billion) and food, agriculture, water and bioeconomy (3.8 billion). Space (1.7 billion) is under the industrial leadership title. Excellent science encompasses various aspects of basic research.

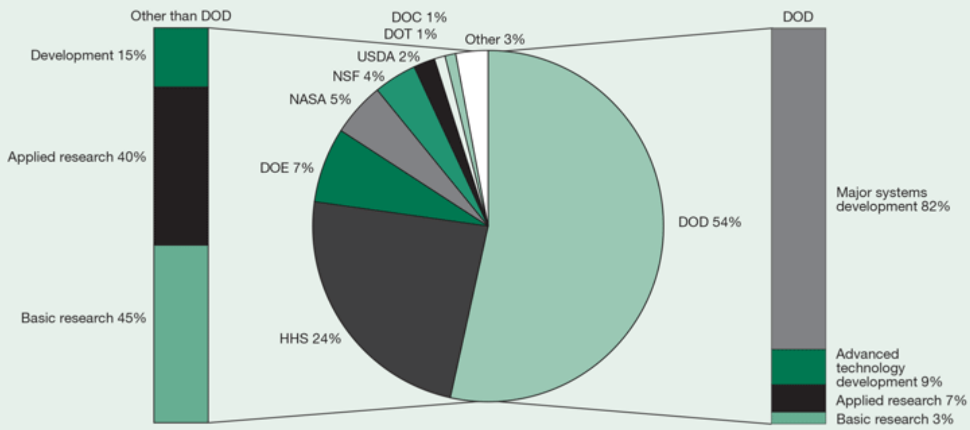
US Federal Research Program

Taken out of the AAAS database, the US budget for research and development shows a drop although a small one over the last 5 years. It's mainly the defense budget that bears the loss.

Research Budget billion $	2010	2011	2012	2013	2014
Defense	92.7	87.2	81.1	70.8	70.5
Non-Defense	67.2	64.1	65.7	62.6	65
Total	159.9	151.3	146.8	133.5	135.5
% total federal budget	4.1	4.0	3.9	3.8	3.4

Research appropriations are distributed to the various US Departments. The figure below shows the R&D breakdown to the major Departments for 2011.

Figure 4-19
Federal obligations for R&D, by agency and character of work: FY 2011



DOC = Department of Commerce; DOD = Department of Defense; DOE = Department of Energy; DOT= Department of Transportation; HHS = Department of Health and Human Services; NASA = National Aeronautics and Space Administration; NSF = National Science Foundation; USDA = U.S. Department of Agriculture.

NOTE: Detail may not add to total due to rounding.

SOURCE: National Science Foundation, National Center for Science and Engineering Statistics, Federal Funds for Research and Development (FYs 2010–12). See appendix table 4-35.

Science and Engineering Indicators 2014

The situation hasn't changed significantly since then. This figure also shows the breakdown in basic research, applied research and development (advanced technology development in DOD). From the picture it becomes clear that US R&D federal funding is largely spent for the development of major military system. This explains why industry receives up to 70% of these funds annually, with the academia second with 13.9%. [source: Matt Hourihan, Federal R&D in FY 2015Budget: An Introduction, AAAS].Concerning non-defense, basic research counts for almost half of the funds. Basic research is mainly carried out under the auspices of the National Science Foundation (NSF) and the National Institute of Health (NIH).

The Departments

US departments administer their allocated research appropriation fairly autonomously. Usually departments have their own science directorates and scientific laboratories that serve the department's priorities and in some cases regulatory provisions. Therefore, a great deal of the research appropriations goes to the salaries of the people working there. It is not clear, except for NIH, what amount of these funds is allocated to extramural work (grants, contracts and other awards). Grants are administered by the science directorates of the respective department. Grants are distributed for services such as:

Grants to individuals for carrying out research (mainly universities)
Centers of excellence
System development and testing
Standards and methods development - often in coordination with the National Institute of Standards and Technology (NIST)
SBIR Program (Small Business Innovation Research)

The second largest beneficiary of the research funds after DOD is the Department of Health and Human Services, in which NIH belongs. NIH spends about 80% of its budget on grants, contracts and other awards [source: John F. Sargent Jr, Federal Research and Development Funding: FY2013, CRS Report, 7-570]

Conclusions and Recommendations

The two research programs, EU and US Federal, have been compared as far as possible from information available in the public domain. The two programs exhibit important differences and some commonalities that are highlighted in this section.

- The EU program is administered centrally by the European Commission DG RTD and according to regulation (EU) No 1291/2013. All instruments and provisions for funding as well as the evaluation mechanisms are established in that regulation. The publication of all calls for expression of interest are through one portal: http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/index.html
- The US program is administered by each department separately, with oversight provided by both the executive branch and a network of appropriations committees in the legislative branch.
- The EU funds as shown in the table cover almost exclusively grants to EU's scientists and other stakeholders taking part in EU projects, whilst only 2% of Horizon 2020

goes to JRC (Joint Research Centre) covering also civil servant salaries. The US funds as shown on the table cover salaries of the people working in the science directorates of the various departments, the specific research labs and institutes as well as grants. With exception of NSF and NIH, it is difficult to know the exact amount allocated to grants and contracts.

- The EU program mainly funds collaborative research projects, with all partners treated equally by the sponsor. The mechanism of collaborative research has served well new EU policies and regulations, since it tends to encourage sharing and to promote consensus.
  Only some US contracts have requirements for collaborative research. Those that do require it still have one contractor and don't give contracts to the partners. However, in Small Business Innovation Research (SBIR) proposals and in some other instances, collaboration may be necessary to win a grant or contract.
- The EU programme is fully competitive. The EU engages external experts to peer review and evaluate proposals for Research Funds. The criteria and scoring system are published in:
  http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/pse/h2020-guide-pse_en.pdf
  Only NSF and NIH apply open and transparent peer review evaluation of the proposals submitted to their calls. The other departments may or not apply peer review depending on the departments' science directorate capabilities.
- All EU funded projects are required to have a dedicated website and a description in the publicly available CORDIS database (http://cordis.europa.eu/projects/home_it.html). The Commission does not claim ownership of the results and is not an intermediary for the research undertaken. Interested parties have to contact directly the project coordinator in order to receive more information. A drawback of this is that often results disappear after the termination of the project.
  In the US grant results are published in the Departments' web sites often without reference to the scientist who undertook the research. Questions should be addressed to the department officer in charge of the research topic. NSF maintains a database with summaries and publications of all its awarded projects: http://www.nsf.gov/awardsearch/. The DOE also has a database of peer-reviewed publications originating from its grants and projects: http://www.osti.gov/pages/
  However, not all the various departments maintain such databases.
- In the EU program, the largest beneficiary seems to be academia with almost 50% allocation of the budget in FP7. In the US, the biggest beneficiary seems to be the industry mainly through DOD's major system development program. However, other departments such as DOE and DHS fund system development and testing for department needs through their RDT&E appropriations. This is not the case for the EU, where the term research for pre-commercial procurement was introduced only in Horizon 2020.
- Both programs, EU and US are subject to only limited high-level evaluation, and there are no studies on how and to what extent the programs impact the economy, society, national and international markets and academia.

On the basis of the above analysis some obvious recommendations are:

- The US would benefit from more collaborative research in which a variety of stakeholders are involved in a single project, all partners contractually committed, along with the scientists. This would contribute to reducing the divide between regulator and industry or regulator and citizen interest groups.
- The US departments' research would benefit from more transparency in the distribution of the grants.
- The EU would benefit from more research funds directed towards advanced system development for products and services for future regulatory requirements. This would create new market niches for innovative products.
- Both programs would benefit from developing built-in mechanisms for impact assessment.

Basic Research

EU's Horizon 2020 has entrusted the European Research Council (ERC) to manage its basic research program. Most of the basic research in the USA is coordinated by NSF in basic science and the NIH for medical science. These organisations are structured similarly and have similar goals.

The ERC's mission is to encourage the highest quality research in Europe through competitive funding and to support investigator-driven frontier research across all fields, on the basis of scientific excellence

The NSF mission is to promote the progress of science; to advance the national health, prosperity, and welfare; to secure the national defense; and for other purposes.

The NIH mission is to seek fundamental knowledge about the nature and behavior of living systems and the application of that knowledge to enhance health, lengthen life, and reduce illness and disability

Scientific excellence appears as NSF's core value, whilst "transform the frontiers of Science and Engineering" is one of the goals of the organization. Another core value of NSF is accountability for public benefit, which sort of matches the competitive funding requirement encompassed in ERC's mission. While NSF divides the applications into specific scientific fields with prioritised interests, ERC encourages applications on all fields with the only distinction being the character of work, i.e. starting, advanced, consolidation, synergy research or proof of concept research. Applications are invited from all nationalities as long as the host organization is in the EU (source: http://erc.europa.eu/sites/default/files/document/file/ERC_Work_Programme_2015.pdf) . The vast majority of non-EU researchers applying for the funds are US residents. NSF funds, in its international exchange program, US researchers in the beginning of their careers to work together with ERC grantees (source: http://erc.europa.eu/sites/default/files/document/file/agreement_EC_NSF.pdf).

	Funding Body	Budget 2014	Industry participation
EU	ERC	€1.7 B (17% of H2020 2014-20)	Limited
US	NIH	(~50% of $ 30.15 B)	Limited
US	NSF	$ 7.2 B (24% of all federal basic research)	In Engineering Research Centers
US	DOD	$2.2 B	Yes
US	DOE – BES	$ 1.8 B	Limited
Source: http://erc.europa.eu/facts-and-figures http://www.nsf.gov/about/ http://science.energy.gov/~/media/budget/pdf/sc-budget-request-to-congress/fy-2014/Cong_Budget_2014_Basic_Energy_Sciences.pdf			

The Department of Defense (DOD) funds long-term basic research in a wide variety of scientific and engineering fields with a goal of exploiting new knowledge to enhance- and where possible, transform-future capabilities. The grants are awarded on the basis of relevance for the Department. [source: Report of the Defense Science Board Task Force on Basic Research, January 2012]

The mission of the DOE's Basic Energy Sciences (BES) program is to support fundamental research to understand, predict, and ultimately control matter and energy at the electronic, atomic, and molecular levels in order to provide the foundations for new energy technologies and to support DOE missions in energy, environment, and national security. DOE funds also the majority of US National Laboratories, and has dedicated resources to the construction and operation of scientific user facilities http://science.energy.gov/bes/suf/ .

NIH has a major program for basic research in the life sciences. Eighty percent of NIH's research budget goes for extramural work and this is mainly in the form of grants. NIH has a rigorous peer review system to evaluate proposals. The budget is distributed to the 27 NIH Institutes and centers to be coordinated and fund the various studies. Basic research cuts through all Institutes, ranging from cancer research, to HIV, neuroscience, etc. http://www.nih.gov/icd/

Conclusions and Recommendations

The basic research programs of the EU and the US are different in nature, size and reach.

- EU's program is administered centrally by the ERC, whilst the US program is split among various organisations with NSF being the most important one for non-defense, non-medical research and NIH for medical research.
- ERC's program is not structured according to scientific disciplines, more it aims to support the single scientist to deliver excellent frontier research. Cross-disciplinarity is however one of the criteria on which the proposals are evaluated. Researchers appreciate this extra degree of freedom and many non-Europeans move to Europe in order to benefit from these grants.
- Some US department such as DOD, DOE, Health & Human Services (HHS) (to which NIH belongs), etc. have strong basic research programs that serve the mission needs of the departments.

- The US departments also fund the construction and maintenance of experimental facilities to support research needs. Through the construction of these facilities the departments commit to long-term funding of related projects. Such commitment is missing in the ERC Program. However, Horizon 2020(2014-2020) funds the European Research Infrastructure Program (ERIC) with **€**2.5 B. The term 'research infrastructures' refers to **facilities, resources and related services** used by the scientific community to conduct top-level research in their respective fields, ranging from social sciences to astronomy, genomics to nanotechnologies (source: http://ec.europa.eu/research/infrastructures/index_en.cfm?pg=what).
- Both the US and EU basic research programs are only partially evaluated and it is not clear how the funded research impacts the economy and the society in general.

Both basic research programs in the EU and US would benefit from more collaboration in facility use. Experimental facilities are key for hypothesis testing and for prototype testing of innovative technologies. Both EU and US host unique facilities, which could become more readily accessible to the cross-border scientific community. In some fields scientists don't have an overview of experimental capabilities. A report produced in the framework of ERNCIP (European Network for Critical Infrastructure Protection) has shown that in Europe there is no overview of European experimental facilities in security. The lack of overview leads to outsourcing of experimental work to US facilities, mainly the US national labs [source: C. Pursiainen,P. Gattinesi, European CIP-related Testing Capabilities: Gaps and Challenges, August 2013]. The development of an inventory of facilities with unique capabilities and a common program to using them for hypothesis testing would both benefit the researchers and would contribute to alleviate facility maintenance costs.

As remarked previously both basic research programs would benefit from development of in-built mechanisms for impact assessment.

Security Research

As explained previously, security research in the EU is mainly funded in the framework programs. However, DG HOME also funded projects with limited research through its CIPS (Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks) program for the same period. The following table shows total amounts of security research funds available. Sources of information for both EU and US are: http://ec.europa.eu/dgs/home-affairs/financing/fundings/security-and-safeguarding-liberties/terrorism-and-other-risks/index_en.htm
http://cordis.europa.eu/fp7/security/home_en.html
Source: http://www.aaas.org/sites/default/files/migrate/uploads/tbli064.pdf

	Program	Budget	Number of funded Projects	Industry Participation
EU	FP7-SECURITY Budget	€ 1,4 B Period 2007-13	325 Demonstration Projects 26	80% 100%
EU	DG HOME CIPS	€ 140 M	129	

		Period 2007-14		
EU	Horizon 2020	€ 1,6 B Period 2014-20	In evolution	
US	Homeland Security R&D	~$6.6 B in 2014 $5.5 B in 2012		see next table

Homeland Security R&D funding breakdown in million US dollars is given in the following table.

	FY 2013	FY 2014	Change %
Agriculture	77	232	200
Commerce	164	205	15.3
Defense	2329	2287	-8
Energy	87	197	127.5
DHS	773	1374	185.7
EPA	42	40	-3.8
HHS/NIH	1804/1804	1806/1805	1.3/1.3
NASA	12	12	0
NSF	396	395	0.1
Total	5700	6600	18

DOD's Science and Technology Directorate is the greatest beneficiary of Homeland Security R&D funds. The S&T Directorate's budget breakdown for 2014 is as follows.

	FY2014 Requested (billion $)	2014 Approved
Basic Research	2.2	
Applied Research	4.6	
Advanced Technology Development **Of which DARPA**	5.1 2.9	
Total	11.9	12

The amounts include the salaries of the Directorate's personnel, grants as well as contracts for technology demonstrations and testing. DARPA's funds are almost exclusively salaries for DARPA's personnel and operating costs of the experimental facilities. It is not clear which part of the S&T Directorate's activities funds are covered by the "Homeland Security R&D" funding as opposed to "Defense R&D" funding. The source for the above table is in page3.9 of: http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2014/FY2014_Budget_Request_Overview_Book.pdf

EU's Security Research Program

The objective of FP7's Security theme was to **develop the technologies** and **knowledge for building capabilities** needed to ensure the security of citizens from threats such as terrorism, natural disasters and crime, while respecting fundamental human rights including privacy; to ensure optimal and concerted use of available and evolving technologies to the benefit of civil European security, to **stimulate the cooperation of providers and users for civil security solutions**, improving the competitiveness of the European security industry and delivering mission-oriented research results to reduce security gaps.

Seven titles of activities were funded under FP7.

1. **Security of citizens**: technology solutions for civil protection, including bio-security and protection against risks arising from crime and terrorist attacks.
2. **Security of infrastructures and utilities**: analysing and securing existing and future critical/networked infrastructure, systems and services
3. **Intelligent surveillance and border security**: technologies and capabilities for the effectiveness and efficiency of all systems, equipment, tools and processes and rapid identification systems for border control and surveillance
4. **Restoring security and safety in case of crisis**: technologies for diverse emergency management operations and on issues, such as inter-organisational preparation, coordination and communication, distributed architectures and human factors
5. **Security systems integration, interconnectivity and interoperability**
6. **Security and society**: socio-economic research
7. **Security research coordination and structuring**

Security of Citizens

The issues of study were:

- CBRN Protection
- Explosives
- Intelligence Against Terrorism
- Ordinary Crime And Forensics
- Organized Crime

Security of Infrastructures and Utilities

The issues of study were:

- Cyber Crime
- Design, Planning Of Buildings And Urban Areas
- Energy, Transport, Communication Grids
- Supply Chain
- Surveillance

Intelligent Surveillance and Border Security

Issues of study were:

- Sea Borders
- Land Borders
- Air Borders
- Border Checks
- Intelligent Border Surveillance

Restoring Security and Safety in case of Crisis

Issues are:

- Preparedness, prevention, mitigation and planning
- Response
- Recovery
- CBRN Response

Security Systems, Integration, Interconnectivity and Interoperability
Topics funded were:

- Information management
- Secure Communications
- Interoperability
- Standardisation

Security and Society

- Citizens, Media and Security
- Organisational requirement for interoperability of public users
- Foresight, scenarios and security as evolving concept
- Security economics
- Ethics and Justice

Security Research Coordination and Practice

- ERA-net (a scheme to promote coordination of research at national and regional level in the EU Member States)
- Small and Medium Enterprises
- Studies
- Other Coordination

EURATOM Program

In all Framework programs there is a part dedicated to Nuclear Energy. This part is called Euratom, and in FP7 received a budget of € 2.751 Billion. The budget breakdown was as follows:

EURATOM (2007-2013)	Budget (Million €)
Fusion Energy Research	1947
Nuclear Fission and Radiation Protection	287
Joint Research Centre	517

DG Home's Grants Program

The table shows DG HOME's grants programs and their respective budgets

	Period 2007-2013	Period 2014-2020
CIPS (Terrorism Prevention)	€140 Million	--------
ISEC (Fight against Crime)	€600 Million	--------
External Borders	€1.8 Billion shared management	--------
AMIF (Asylum, Migration and Integration Fund)	€4 Billion	€3.137Billion
ISF (internal Security Fund)-Borders & Visa		€2.760 Billion / 1 Billion direct funding

ISF-Police	€1 Billion/342 Million direct funding

DG HOME's grants program has the objective to promote collaboration among Member States and raise awareness on security issues. It promoted collaboration among authorities, utilities and research organisations or academia. The scope was not research for knowledge generation, but more application of research results and dissemination of current knowledge and good practice. All awarded projects under CIPS can be found in: http://ec.europa.eu/dgs/home-affairs/financing/fundings/security-and-safeguarding-liberties/terrorism-and-other-risks/index_en.htm and of ISEC under: http://ec.europa.eu/dgs/home-affairs/financing/fundings/security-and-safeguarding-liberties/prevention-of-and-fight-against-crime/index_en.htm

Projects may be funded under direct funding scheme, i.e., managed by DG HOME or under the shared management scheme, i.e., managed directly by the Member States. When funded under the shared management scheme, there is no information about how the funds are distributed. DG HOME has set up a web site where information on the funds that each Member State has received can be viewed: http://ec.europa.eu/dgs/home-affairs/financing/fundings/mapping-funds/index_en.htm

Again, all above indicated funds are for grants and contracts only.

DHS's Science & Technology Program

DHS has an in-house scientific capability, the Science and Technology Directorate, whose job is to "*strengthen America's security and resiliency by providing knowledge products and innovative technology solutions for the Homeland Security Enterprise*". The science & technology for the radiological/nuclear threat within DHS is handled by a separate group, the Domestic Nuclear Detection Office.

According to http://www.dhs.gov/sites/default/files/publications/MGMT/FY%202014%20BIB%20-%20FINAL%20-508%20Formatted%20(4).pdf the budget breakdown is:

	FY 2014 requested (Million $)	FY 2014 approved (Million &)
Management & Administration	129.6	
Acquisition & Operations Support	41.7	
Laboratory Facilities	857.8	
Research, Development and Innovation	467	
University Programs	31	
Total	1500	1374
Domestic Nuclear Detection Of.		291.3

DHS S&T maintains a system of laboratory facilities, which have unique capabilities for specific threats:

- Chemical Security Analysis Center (CSAC) Its mission is to identify and assess chemical threats and vulnerabilities in the United States and develop the best responses to potential chemical hazards.
- National Biodefense Analysis and Countermeasures Center (NBACC) Its mission is to defend the nation against biological threats.
- National Bio and Agro-Defense Facility (NBAF). Its mission will be (proposed lab) to study foreign animal, emerging and zoonotic diseases that threaten the US animal agriculture and public health.
- National Urban Security Testing Laboratory (NUSTL) Its mission is to support the successful development, evaluation and transition of homeland security technologies into field use for law enforcement, fire and other emergency response agaencies.
- Plum Island Animal Disease Center (PIADC) Its mission is to work on high-consequence, live foot-and-mouth disease.
- Transportation Security Laboratory (TSL). It offers the homeland security community the ability to advance detection technology from conception to deployment through applied research, test and evaluation, assessment, certification and qualification testing.

The DHS S&T HSARPA (Homeland Security Advanced Research Project Agency) is also beneficiary of this budget. The work program 2014 of HSARPA included the following:

Borders and Maritime Security

- Cargo
- Land
- Maritime

Chemical and Biological Defense

- Threat Awareness
- Biosurveillance
- Detection and Diagnostics
- Response and Recovery

Cyber Security

Explosives

- Air Cargo
- Aircraft Vulnerability
- Canine Detection
- Checked Baggage
- Checkpoint
- Homemade Explosives
- Mass Transit
- Standoff Detection
- Trace Detection

Resilient Systems

- Community Resilience
- Critical Infrastructure
- Cyber Physical Systems
- Decision Support
- Evaluation Research
- Security and Identification

Nuclear Security in the US

The National Nuclear Security Administration is the main organization charged for nuclear security in the US. Their budget in 2015 was $11.4 billion. Their priorities include effective stewardship of the nuclear deterrent, controlling and eliminating nuclear materials worldwide, advancing navy nuclear propulsion, and strengthening key science technology and engineering capabilities (source: http://nnsa.energy.gov/aboutus/budget).

The Domestic Nuclear Detection Office in DHS is in charge of implementing domestic nuclear detection efforts for a managed and coordinated response to radiological and nuclear threats, as well as integration of federal nuclear forensics program (source: http://www.dhs.gov/about-domestic-nuclear-detection-office).

Comparison of Security Research

Since EU's framework programs are not concerned with either defense or medicine, the security part of FP7 (without the Euratom research) can best be compared with DHS's Science and Technology Directorate.

Comparative table EU-FP7and US-DHS Security Research

EU-FP7-security	US-DHS-S&T	Comment
CBRN Protection CBRN Response*	CBRN Threat Awareness Biosurveillance Detection and Diagnostics Response and Recovery	The DHS program covers more aspects. * Under crisis management in the EU
Explosives	Explosives	Both programs are comprehensive
Intelligence	--------	IARPA is in charge of this in the USA
Ordinary Crime Organised Crime	---------	Not under DHS
Cyber crime	Cyber security	Cyber security is dealt in Europe by DG CONNECT only Cybercrime under Security
Euratom	Domestic Nuclear Detection Office	DOE has the National Nuclear Security Administration

Concerning Borders the comparison reveals:

EU-FP7-security	US-DHS-science	Comment
Land Border	Land Border	
Sea Border	Maritime Border	
Air Border	Air-based Technologies*	*Under Land Border in the US
Border Checks	Checkpoints*	*Under Explosives in the US
Supply Chain*	Cargo Security	*Under Infrastructure in the EU
Intelligent Surveillance	In each HSARPA portfolio	Under Land, Maritime and Cargo in the US

Concerning Crisis Management and Resilience the comparison reveals:

EU-FP7-security	US-DHS-science	Comment
Preparedness, prevention, mitigation and planning Response and Recovery	Cyber Physical Systems Decision Support Identification Evaluation First Responders technologies	
Energy and Transport grids	Critical Infrastructure	The US program goes beyond energy and transport
Design, Planning Of Buildings And Urban Areas	Community Resilience	The US program goes beyond Buildings and Urban areas

Concerning horizontal issues the comparison reveals:

EU-FP7-security	US-DHS-science	Comment
Information management Secure communications Interoperability Standardisation	Interoperability and Compatibility System Assessment and Validation Capability Development	Capability development includes the Standards office and the Operational Test and Evaluation office

Concerning social & stakeholders issues:

EU-FP7-security	US-DHS-science	Comment
Citizens, Media & Security Organisational requirement for interoperability of public users Foresight, scenarios & security as evolving concept Security economics Ethics and Justice	Communication Office Interagency Office International Cooperative projects office Office of Public Private Partnerships Office of University Programs*	*University Programs are about Excellence centres and development of Security-related university curricula and training

The EU-FP7-security SME (small medium enterprise) program is comparable to the US-DHS-science SBIR (small business innovation research) program.

The Future in Security Research

The strategic goal of DHS S&T's APEX programs is to look at the nation's security and address future challenges while continuing to support today's operational needs. Priorities of APEX are:

- APEX Entry/Exit Re-engineering to increase Customs and Border Protection's capacity to screen travelers entering the United States and to confirm the departure of non-U.S. citizens from U.S. airports.
- APEX Next Generation First Responder with the aim to develop a scalable and modular ensemble that includes an enhanced duty uniform, personal protective equipment, wearable computing and sensing technology, and robust voice and data communication networks.
- APEX Screening at Speed with the aim to create an almost-invisible checkpoint by integrating imaging, trace detection, X-ray technologies, and software systems.

In EU's Horizon 2020, one of the topics in the call "Disaster Resilience: Safeguarding and securing society, including adapting to climate change" is about improving the aviation security chain:
http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/1075-drs-16-2014.html .
Possible areas of research (not exclusive) for this call could be: "alternative screening processes and interventions; investigate how, where and when aviation security controls shall take place to provide the most effective and efficient results; look at the further development of processes' to maximise security outcome and minimise impact on industry and passengers; and how compliance and their effectiveness will be demonstrated. It should include system level solutions"

Another topic in the same call is about "Communication technologies and interoperability topic 2: Next generation emergency services" source:
http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/1077-drs-19-2014.html .
The call asks for "..build a validation-focused programme/framework using existing standards and protocols, with consideration of e.g. call location and routing, video calling to assist people with disabilities, security, integration of social media channels Next Generation eCall, messaging and early warning systemsetc". It requires "European technology providers, emergency services organisations, research and development laboratories, telecommunication network providers, Voice Over IP providers, and software providers to build on the expertise in a collaborative fashion".

Conclusions and Recommendations

- The two programs look quite similar in terms of objectives, priorities and subjects treated. Both programs have a strong technology development angle. Both institutions vastly involve the security industry in the development of technology.

Whilst FP7 engages the industry and the scientists in the collaborative research scheme, DHS provides its own scientists to guide the industrial development.

- The bottom up approach of EU's security research serves well to develop a shared base of knowledge, to exchange good practice and arrive to consensus. However it lacks leadership to capitalize on the above achievements. DHS's S&T provides leadership to develop the technologies and knowledge needed for the "homeland security enterprise" but might not always be shared by the economic and social stakeholders.
- DHS S&T gathers the technology requirements of the many DHS operational components, such as FEMA, TSA, Coast Guard, Customs and Border Protection, etc. to guide procurement of suitable solutions. S&T goes beyond existing solutions and stimulates the industry to develop the next generation products, which then will be most probably acquired by future DHS procurements.
- In the EU, security procurements remain the responsibility of the Member States. After developing their products through EU research, companies are left on their own to find their way to a fragmented EU public procurement process.
- Despite the enthusiasm of industry and scientists to develop innovative products, often the technology training of authorities, utilities and other service providers is low. Utilities show little understanding for the additional costs of innovation in security. This is valid for both the EU and US communities.
- DHS S&T has its own laboratories to obtain advice on the best technology standards and state of the art knowledge in security. In the EU the access to labs is limited. First because the experimental capabilities of the Member States are not well understood and networked, and second because the security topic has only recently entered the research framework program. DG HOME's ERNCIP project has the aim to network EU's experimental facilities to obtain advice and standards (https://erncip-project.jrc.ec.europa.eu).
- DHS S&T has launched its academic program, with the aim to develop proper security training and certification for professionals for all economic sectors. Neither DG HOME nor Horizon 2020 (FP7's successor) have set that goal.
- DHS capitalizes on NIST's (National Institute of Standards and Technology) extensive experimental capabilities and industrial networks to extend its standardization program and guide the trading of security solutions in other economic sectors in the US and externally. The EU does not have a similar organization to NIST. JRC provides some support for measurement standards, but JRC's mandate in standardization remains limited to the urgent needs of policy that require CEN/CENELEC intervention. NIST's mandate is the competitiveness of the US industry by advancing standards and measurements. NIST standards experts are not necessarily involved in ANSI's (American National Standards Institute) standardization program, but provide a measurements and standards base for ANSI standardization. In the EU, much of the work that NIST does would be characterized as pre-norms, given that the word *standard* is reserved for the formal process of recognized standardization bodies.

Pre-normative work at the EU level should be strengthened. This could be achieved by networking EU's laboratory capabilities and Member States authorities under strong leadership, provided by DG HOME. A program of lab funding could support the network to use their resources for harmonization of test protocol, certification, reference materials and training as well as benchmarking and research. Once tested equipment may be cleared for procurement from all EU Member States. A model procurement of security equipment could be developed similar to the one currently used for defense under Directive 2009/81/EC on defense and sensitive security procurement http://ec.europa.eu/growth/single-market/public-procurement/rules/defence-procurement/index_en.htm

The EU should support the development of academic courses and curricula on security of critical infrastructures at all levels. The industry should be involved in developing the curricula since they will be the beneficiaries of better security trained staff. Such an activity has been taken up by ERNCIP and should strengthened in the future https://erncip-project.jrc.ec.europa.eu/networks/academic-committee/63-academic-committee-news/137-3rd-erncip-academic-committee-meeting-on-20-21-october-2014-in-ispra

Case Study CBRN Research

Scientific research in both EU and US is very much driven by the respective CBRN policies.

US CBRN Policies

In the US, mainly 4 departments share the CBRN research budget, HHS, DOD, DHS and EPA with lesser amounts going to DOJ's FBI and the USDA.

Programs	2015 Budget ($)
HHS BioShield and BARDA	415 and 415 million
DOD Chemical Biological Defense	1.4 billion
EPA	33.8 million
DHS S&T	125.426 million.
Source http://www.hhs.gov/budget/fy2015-hhs-budget-in-brief/hhs-budget-in-brief-phssef.html http://www2.epa.gov/sites/production/files/2014-03/documents/fy15_bib.pdf https://www.dhs.gov/sites/default/files/publications/DHS%20S%26T%20Research,%20Development,%20Acquisition%20and%20Operations%20Fiscal%20Year%202015%20Congressional%20Justification.pdf	

HHS is the coordinator of medical countermeasures and the BioShield project, under which the national vaccine stockpile is created. At the same time, HHS hosts the agency BARDA (Biomedical Advanced Research and Development Authority), whose role is to fund and coordinate research on CB countermeasures. BioShield spent $ 3.3 billion in the period between 2003-2013, 90% of which was spent for the development of vaccines for *Bacillus anthracis* (anthrax), smallpox and botulism. In 2015 the US Congress has agreed to spending $ 415 million for BioShield and another $ 415 million for BARDA. BioShield is a coordinated effort between BARDA, NIH, American Pharmaceutical Industry and FDA for: vaccine development, testing, licensing and acquisition. Big Pharmaceutical Industry has not been positive about vaccine development since they don't see a market beyond the national stockpile. Moreover,

clinical testing is also time consuming and expensive and liabilities are high. In order to get some participation at all, the congress had to remove liabilities for the developed vaccines from the companies due to limited testing or non-human clinical testing. Liabilities to the industry involved in the BioShield project have been removed.
http://www.hhs.gov/budget/fy2015/fy2015-public-health-social-services-emergency-budget-justification.pdf

Many contracts have been given to smaller companies, though some failed to either develop or produce the countermeasure in the given time limit. Vaccines are considered biological products. For such products FDA licenses the products. Issuance of a biologics license is a determination that the product, the manufacturing process, and the manufacturing facilities meet applicable requirements to ensure the continued safety, purity and potency of the product. Since licensing by FDA takes some time, often countermeasures have started stockpiling before licensing. According to law, the Secretary of Health has the right to authorize the use of countermeasures even without licensing in case of crisis.

The DOD similarly develops medical countermeasures for its combat troops. DOD's threat list is different than the national security threat list. DOD does distribute provisionally vaccination to soldiers with CBRN at risk missions. Budget is summarized in the sources below, for RDT&E and procurement.
http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2015/budget_justification/pdfs/03_RDT_and_E/4_RDTE_MasterJustificationBook_Chemical_Biological_Defense_Program_PB_2015_Vol_4.pdf
http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2015/budget_justification/pdfs/02_Procurement/PROCUREMENT_MasterJustificationBook_Chemical_and_Biological_Defense_Program_PB_2015_1_3.pdf

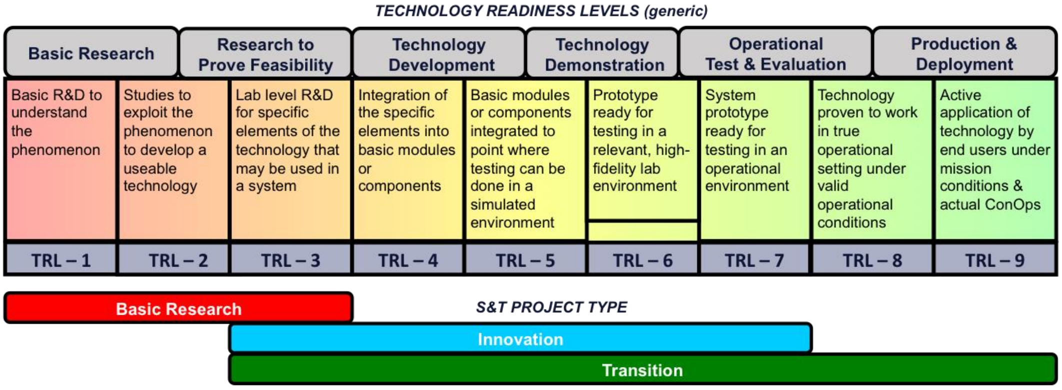
Moreover DOD's Chemical Biological Defense program includes the development and production of handheld CBRN detection devises, protective cladding and decontamination devices for combat troops. A great deal of this research and development spills over to homeland security applications. Biowatch of DHS Office of Health Affairs is a project which aims to equip the US transportation sector with bio detectors. Biowatch-3 cost $61 million between 2009 and April 2014, when DHS cancelled the acquisition. The program failed to produce what it envisioned to become "lab-in-a-box". Nevertheless DHS stays committed to continue efforts in that field.
Source:
http://www.nationaldefensemagazine.org/archive/2014/June/Pages/BioWatch3Ends,ButNot%E2%80%98Lab-in-a-Box%E2%80%99Goal.aspx

Major contracts to US industry by DOD and DHS have stimulated the development of technologies, but these have been slow to be absorbed by homeland security actors such as utilities, civil protection and police. The National Strategy for CBRNE Standards tried to tackle this problem. DHS, DOD and EPA in collaboration with NIST support activities for the development of standards in such technologies in order to make them more functional and affordable for users.
http://www.dhs.gov/sites/default/files/publications/DHS%20S%26T%20Research,%20Development,%20Acquisition%20and%20Operations%20Fiscal%20Year%202015%20Congressional%20Justification.pdf

Nevertheless development of both solutions and standards have been slow in the US and even slower in the EU.

DOD's Technology Acquisition Model

As mentioned previously technology in CBRNE is mostly acquired through DOD's acquisition methods. This model is also followed by DHS but in a much smaller scale. DOD also uses a methodology to define technology readiness levels for new system development (http://www.dtic.mil/ndia/2003systems/nolte2.pdf) (see picture).



A successful technology will be followed the whole way through up to acquisition and deployment by DOD .

According to a report from the Congressional research service: "Defence acquisitions: how DOD acquires weapon systems and recent efforts to reform the process" by Moshe Schwartz, http://fas.org/sgp/crs/natsec/RL34026.pdf, DOD's technology acquisition model also includes technology design and development. It is a full cycle starting from DOD's streamlined user requirements to system requirement, design, development, testing, production and acquisition. It is a long-term process, sometimes over decades. Usually the result is a highly customized solution, whose development and production bears no risk for the industry since the sponsor, DOD, will also be the customer. However, according to the above mentioned report this method presents many difficulties.

Usually there is one main contractor to develop a highly sophisticated solution. The contractor may have subcontractors, but the prime contractor is the program executor. There are no requirements for consortia building and sharing of work, responsibilities and decision making.

The contractor is in constant dialogue with the sponsor and customer, i.e., the DOD. However DOD's input and involvement depends on the capabilities and knowledge of the limited federal program officers that will work on the project. Of course DOD has a pool of high profile scientists in its ranks to draw from and the process is well monitored. Nevertheless, the number of contracts that DoD has is huge and the in-house scientific resources are limited.

Defense acquisition processes usually require much more money and need much more time than originally estimated. This is due to factors including limited in-house scientific personnel, but also to the nature of the process. The defense industry has no pressure to meet market's requirements, only DOD's requirements. By funding such large acquisition projects the US government acts as both customer and regulator, thereby skewing free market rules. Last but not least, industry has a no risk attitude. Companies don't innovate unless they are engaged in such an acquisition program. This is true for big industry that usually receives these contracts. The situation is different for small and medium industry (SME or SBIR), who do innovate but face limits on bidding on DOD's huge contracts. The only mechanism DOD has to involvement in the acquisition process is through subcontracting of the main contractor. This cuts out SBIRs from decision making and visibility.

Differences with Horizon 2020

HORIZON 2020 also applies Technology Readiness Levels and in each call they are clearly mentioned. However it is the consortium that should commit to the technology development and not the customer. Often there is no potential customer involved in the consortia. Security Technology developed may be never tested, if tested may be never applied operationally, if operational may never be acquired. Testing protocols of the technology and operational requirements hardly go beyond the project. There are no EU wide operational requirements, testing protocols and good practice repositories.

If the technology in the end does find its way to a customer in a EU Member State by no means it is launched in the full European Market, due to a lack of a single market for security. The technology would have to be approved and re-approved in every single Member State before acquisition. The pre-commercial procurement mechanism has been launched in order to support this transition but is still to be fire tested.

EU CBRN Policies

The main policy document on CBRN is the EU's CBRN action plan. It's strategic goal is to reduce the CBRN threat in Europe; it consists of 124 actions in order to achieve the goal, starting from enhancing security of high-risk material and security to improvement of information exchange among Member States and to standards for detection equipment. Research at EU level is designed in support of these actions.
http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/explosives/docs/20140505_detection_and_mitigation_of_cbrn-e_risks_at_eu_level_en.pdf

However, some other EU policy documents mention CBRN threats and invoke measures to protect the public. These are summarized in the table below.

DG	Policy	Comment
HOME	CBRN Action Plan (2009)	
ECHO	Civil Protection Mechanism (2001)	Civil protection exercises on CBRN

ENV	SEVESO III Directive (2012)	On protection of chemical plants
SANCO	Decision on Cross-border threats to health (2013)	Includes joint procurement of medical countermeasures
EEAS	Chemical Weapons Convention, Biological Weapons Convention	
ENER	Framework for Nuclear Safety of Nuclear Installations (2014)	Regulated as RN material source
MOVE	Guidelines for Trans-European Transport Network (2014)	CBRN threats are not mentioned, however legislator keep an eye on them
GROWTH	EU security industrial policy (2012)	Mandate 487 for CBRN-E standards

EU's Research on CBRN-E

EU's research budget covers also explosives research. During FP7 (2007-2013) there were funded 60 CBRN projects worth 200 million and 15 projects worth 67 million. Examples include:

Acronym	Description	Budget □	# Partners
SECUR-ED	Demo security technologies incl. CBRN detection	40 M	40
EDEN	Demo CBRN Resilience	36 M	37
CATO	CBRN crisis management	14 M	27
PRACTICE	Preparedness and Resilience against CBRN terror attack	12.7 M	26

The partners from institutions all over Europe include academia, industry, research organisations, non-profit organisations, and local and Member State regulatory authorities.

Calls with CBRN-E content will continue in Horizon 2020. There has been already an open call with the title "Tools for detection, traceability, triage and individual monitoring of victims after a mass CBRNE contamination or exposure" which closed in 28/8/2014. The call asked for "...improved CBRN detection and monitoring capabilities..." and that "..existing networks of users (defense/security experts, firemen, rescuers) are actively involved...". Budget preferably between €5-12m.

A call with deadline 27/08/2015 stated "....addressing standardisation opportunities in support of increasing disaster resilience...". This call asks for this research to be carried out within the context of policy initiatives such as the CEN/CENELEC/ETSI Mandate 487 for the development of security standards (CBRNE, Crisis Management and Border Security) and in collaboration with CEN/TC 391 and ISO/TC 223.

The Joint Research Centre's ERNCIP (European Reference Network for Critical Infrastructure Protection), which aims at the development of security pre-norms and recommendations for Critical Infrastructure Operators and authorities all over Europe, received direct funding from Horizon 2020 over the years 2014-15, for supporting the work of the mandate 487 to CEN/CENELEC and ETSI.

JRC also leads the development of the COEs (Centres of Excellence) in CBRN. An effort to prepare and transfer knowledge to developing counties on CBRN threats and counter measures. 51 countries host such Centres of Excellence today. Many of the Countries develop their national CBRN strategies as a result of EU's COE work. Source: http://www.cbrn-coe.eu

Security Standards

The US Standards Communities

NIST is a catalyst for US standards. NIST's mission to promote US innovation and industrial competitiveness by advancing measurement science, standards and technology and its core competences in measurement science standards development and use, give it a key position worldwide. Its internationally recognized expertise comes from its wide base of laboratories and experimental programs.

NIST supports US agencies to understand and work with advanced technology to improve technical requirements of their procurement processes. NIST experts lead technical discussions on standardization, support the industry with data and lab work, and bring along scientific insights important for the advancement of technologies appreciated by both the industry and the public procurer. NIST maintains extensive public databases of all sorts of recommendations and guidelines for the proper use and testing of technology.

NIST has been working with the other federal agencies, industry stakeholders and standards development t organizations to develop standards, test methods and conformity assessment systems for CBRN equipment for first responders. The types of equipment range from detectors, to protective ensembles and respirators, to sampling and decontamination technologies.

The table below summarizes the standards and conformity assessment procedures that have been developed for hand-held detectors for CBRN agents. The situation with performance standards is fairly good. However, test methods to show conformity with standards still lag behind. In most cases testing is still carried out in specialized DOD facilities.

Threat	Standard	Conformity Assessment	Method
Chemical	ASTM 2885-13	None	Ion Mobility Spectrometry (IMS)
Biological	AOAC Standard Method Performance Requirements	AOAC International (Very limited)	Polymerase Chain Reaction (PCR)
Radiological / Nuclear	IEEE/ANSI N42.34 and N42.48	DNDO GRaDER	Neutron Detection & Gamma-Ray Spectrometry

Some observations and lessons learned from substantial US investments in CBRN standards and conformity assessment are:

- For chemical and biological agents, detection is critically dependent on how the sample is taken. The detection technology may be quite sensitive, but the sample must be introduced into the detection volume.
- The research agenda in related fields can drive the technology development. Biotechnology, for example, continues to develop more sensitive and specific methods of detection traces of biological agents and this technology is directly relevant to detection of biological warfare agents.
- NIST participation and leadership of the standards writing groups are essential to both development of the standards and their buy-in from the users.
- After a decade of use of this class of detectors, there are increasing efforts to harmonize standards for CBRN detection systems. As markets continue to expand, there is greater acceptance of standards by both federal agencies and US industry.

Stakeholders involved in the standardization process acknowledged the importance of the contribution of NIST's laboratory work and expertise. Furthermore NIST gave the stakeholders important insights on how to improve both the technology and the requirements.

The EU Standards Communities

The EU's standardization efforts in CBRN haven't gone very far. Horizon 2020 is a great mechanism to produce CBRN technology, but it hardly finds its way to public procurement and to standardization.

JRC's ERNCIP is a completely bottom up and voluntary network for the preparation and development of security pre-norms. It is active in the fields of:

Chemical Biological threats in Water
Explosive detection in sectors other than aviation
Radiological and Nuclear threats
Structural resistance to explosions

In each of these fields, stakeholder groups are convened, led by champion scientists, to exchange laboratory good practice and develop pre-norms. Examples of the groups' work are:

- List-mode data acquisition based on digital electronics (EUR 26715). Pulse processing digitisers are powerful instruments, important for nuclear security, critical infrastructure protection, nuclear physics and radiation metrology. Some critical parameters affect their performance in both lab and field. Tests are proposed to assess the performance of acquisition systems for these parameters.
- Protocols for more efficient cooperation between competent authorities and remote expert support or reachback centres at the national and international level, for radiation measurements and data analysis.
- Review of methods for the rapid identification of pathogens in water samples.

More details can be found in https://erncip-project.jrc.ec.europa.eu/download-area/viewcategory/8-thematic-groups

Some of these pre-norms can be taken up by Technical Committee 391 of CEN/CENELEC to become EU standards. This process will require another 3-5 years. In the meantime industry that wants to develop products as well as public authorities that need to procure products may use ERNCIP's pre-norms. The European single market sorely needs such pre-norms to operate properly for all possible technology solutions and even more so for security technologies such as CBRN. Other Research Framework Projects would have developed such pre-norms, if there were a possibility to file them in a common repository, where they could be accessed by interested parties. JRC could play a role in collecting and maintaining a systematic repository of approved pre-norms and recommendations for public procurement.

The International Security Standards

The international standards for CBRN countermeasures most recognized are those produced by the International Organisation for Standards (ISO) and the International Electrotechnical Commission (IEC). The ISO and IEC technical committees, subcommittees and working groups sometimes develop standards, but often use as a starting point a national standard submitted by a member from the US or an EU Member State, as well as contributions from other member nations.

CBRN technologies have evolved rapidly over the past two decades and the measurements and standards infrastructures differ markedly for different technologies. The ISO in 2014 established a new umbrella Technical Committee (TC 292) to collect different ISO TC activities that focus on security standards. The international members of this TC represent important stakeholder communities in the US and EU for standards in emergency preparedness and resilience. This activity could in future include standards for operational response to CBRN incidents.

Performance standards for specific technologies, on the other hand, are often developed by IEC technical committees. A good example is the standards for radiological/nuclear detectors and x-ray scanning systems developed under IEC TC 45.

There are other important standards for security technologies developed by US domiciled standards development organisations that have international including EU members as active participants. These include, for examples, ASTM International (chemical, biological and explosives), AOAC International (microbiological). ASTM and AOAC standards are sometimes, but not always, submitted to ISO for consideration as international standards.

Recommendations and Conclusions

US CBRN technology development would benefit from a higher participation of small and innovative companies, to stimulate competition within the industry and better products with less cost.

The EU's security and CBRN single market would benefit from a mechanism for identifying pre-norm activities underway in both communities. And, for some common repositories for cataloging the pre-norms and subsequent standards for the security technologies. Horizon 2020 and JRC could be part of this mechanism. Possible models include security standards databases prepared by the US American National Standards Institute (ANSI) and the International Organisation for Standards (ISO).

http://www.hssd.us/

http://www.iso.org/sites/sags/

Conclusions and Future Work

The EU and US research influence on industrial competitiveness has been analysed at high level. Important differences have been pointed out in the operation of the budget distribution. These differences become more important in the field of security and CBRN in particular. The collaborative scheme of EU's research favors pluralism and small business but it lacks committed customers. On the other hand standardization and testing and evaluation is more successful in the US through a well-funded laboratory network, NIST and a faster standardization routine in comparison to the EU. Future work should look in more detail on how to further exploit collaborative research for the purpose of technology acquisition and how to boost EU's standardization and testing and evaluation mechanism to better serve the single market's needs. A central repository of best practice, technical guidelines and testing protocols as produced by EU's Horizon 2020, would be a cornerstone for the single market and the EU industry. JRC could be the host of such a repository.

LB-NA-27403-EN-N

JRC Mission

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new methods, tools and standards, and sharing its know-how with the Member States, the scientific community and international partners.

Serving society
Stimulating innovation
Supporting legislation

doi:10.2788/082867

ISBN 978-92-79-50547-8

Publications Office