2014 U.S.–U.K. Program on Collaboration on Resiliency and Security (ColoRS) Working Meeting

Science & Technology Facilities Council

Homeland Security
Science and Technology

US-UK COLLABORATION ON RESILIENCE AND SECURITY

SUMMARY REPORT FROM NOVEMBER 17-18, 2014, WORKING MEETING

WASHINGTON, D.C.

CO-HOSTED BY:

US Department of Homeland Security, Science and Technology Directorate

UK Science and Technology Facilities Council

Homeland Security
Science and Technology

Pacific Northwest
NATIONAL LABORATORY

Science & Technology Facilities Council

DISCLAIMER

2014 U.S.–U.K. Program on Collaboration on Resiliency and Security (ColoRS) Working Meeting

Science & Technology Facilities Council

Homeland Security
Science and Technology

US-UK COLLABORATION ON RESILIENCE AND SECURITY

SUMMARY REPORT FROM NOVEMBER 17-18, 2014, WORKING MEETING
WASHINGTON, D.C.

CO-HOSTED BY

US Department of Homeland Security, Science and Technology Directorate (DHS S&T)

UK Science and Technology Facilities Council (STFC)

AUTHORS AND EXECUTIVE PLANNING TEAM

Bryan Edwards
Security and Resilience Futures, STFC

Linda Enderby
Futures Team, STFC

Joseph Kielman
Cyber Security Division, DHS S&T

Emily Saulsgiver
Contract Support to DHS S&T

Ann Lesperance
Pacific Northwest National Laboratory

Jessica Sandusky
Pacific Northwest National Laboratory

Homeland Security
Science and Technology

Pacific Northwest
NATIONAL LABORATORY

Science & Technology Facilities Council

"From a cybersecurity perspective, we need to identify research needs and encourage multi-domain and multi-disciplinary teams to better anticipate threats to cyber infrastructure and mitigate the impact infrastructure failures would have on our societies. It is through collaborations like ColoRS that we are able to amplify our individual efforts and find shared solutions to combat these challenges."

Dr. Douglas Maughan, Director, Cyber Security Division, DHS S&T

CONTENTS

EXECUTIVE SUMMARY

For the past ten years, the US Department of Homeland Security Science and Technology Directorate (S&T) and the UK Home Office have encouraged and supported a variety of joint engagements related to research and development in support of homeland security. The goal has been to develop longer-term strategic collaborations with partners that have complementary interests. This relationship was formally expanded to include the UK Science and Technology Facilities Council (STFC) in 2013. STFC and S&T launched the US-UK Collaboration on Resiliency and Security (ColoRS) program to identify areas of mutual interest related to resilient critical cyber or societal infrastructures, which will lead to further collaborative focus and research.

Through ColoRS, S&T and STFC held an invitational working meeting on November 17 and 18, 2014, in Washington, D.C., to focus on three themes:

1. Securing infrastructure from cyber disruptions
2. Modeling and measuring societal resilience
3. Analytics for effective data exploitation.

The structure of the ColoRS working meeting was experimental in design with the goal of bringing together experts in diverse fields to collaborate on the topics of cybersecurity and the impact on social structures during a cyber-crisis. Invitees to this working meeting compromised UK and US researchers from the federal government, national laboratories, universities, and response community. Invitee backgrounds ranged from cyber infrastructure to epidemiology and medicine to mathematics and social science. Infrastructure owners and law enforcement personnel were also included to ensure discussions stayed grounded in mission needs and assumptions were vetted by public safety practitioners. This report documents the ColoRS meeting discussions and the research areas identified for further exploration.

Participant Feedback: "Wonderful balance of creative communication, brainstorming, and focused work on a meaningful product."

The meeting resulted in three outputs:

- A multi-disciplinary narrative of the problems, recognizing the deficiencies in current analyses
- A list of research questions and issues
- Concepts needed to address questions.

Concepts are currently being further developed by the participants and range from ways to factor the human element into resilient system design to the unique aspects of restoring cyber infrastructure and social networks following a cyber-attack. Participants will prepare the concepts and submit them as papers for inclusion in a book to be published by Elsevier in September 2015. STFC is coordinating the publication of the book with editors from STFC and S&T.

The partnership between the UK and the US is an important one for several reasons. It brings together the two nations' collective experience and knowledge. It allows us to share specialists and techniques and develop much-needed novel solutions. It enables us to unify standards and understand how to use technology in a unified world. We can work together in times of emergencies and prepare more effectively for them."

Prof. Bernard Silverman, Chief Scientific Advisor to the Home Office, UK

INTRODUCTION

A large-scale cyber-attack will cause a disaster not only in critical infrastructure failure but also societal collapse in this digitally connected age. How do we understand such disasters? How can we prepare? How do we better understand the interdependencies of critical infrastructure and social resilience? How can we mitigate, limit the extent, and ultimately restore society to some level of functionality and safety? Experts fear that existing techniques to understand technical and societal consequences of a cyber-disaster are insufficient, and we lack approaches to examine the interconnections. A multi-disciplinary approach might lay out the landscape and identify ways to meet these needs.

The US Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Cyber Security Division (CSD) is working with the UK Home Office on a number of joint cybersecurity efforts to enable cost-sharing, shared intellectual property rights, and joint access to project results. This US-UK bilateral relationship was formed ten years ago when DHS was first established as a department of the US government. Collaborations under the US-UK bilateral agreement take place within Project Agreements and Information Sharing Annexes. The CSD engagements consider technical topics, such as insider threat, national critical infrastructure security, big data, and cyber forensics. The overall intent is to develop longer-term strategic collaborations with partners that have complementary interests to help ensure the maximum impact and value. As an extension of this relationship, in 2013, DHS S&T and the UK Home Office signed an Information Sharing Annex to support a joint program called Collaboration on Resiliency and Security (ColoRS).

US and UK Organizers, Sponsors, and Plenary Speakers of the ColoRS working meeting included (from left to right) Joseph Kielman (Chief Scientific Advisor, CSD, DHS S&T), Bryan Edwards *(Defence, Security and Resilience Theme Lead, Futures Programme, STFC), Bernard Silverman (Chief Scientific Advisor, UK Home Office), Robert Griffin (Deputy Under Secretary, DHS S&T), Douglas Maughan (Director, CSD, DHS S&T), Emily Saulsgiver (contract support to DHS S&T), Linda Enderby (Stakeholder Management, STFC), and Iain Williams (Counselor, Security and Counter Terrorism Science and Technology, UK Home Office)*

ColoRS is a collaboration between CSD and the UK Science and Technology Facilities Council (STFC). The purpose of this program is to identify areas of mutual interest related to resilient critical or societal infrastructures, which will lead to further focus and research. On November 17 and 18, the two agencies held a ColoRS working meeting in Washington, D.C. It was the first meeting of this type under the US-UK bilateral agreement, increasing engagement among US and UK researchers to examine techniques and technologies that might inform our understanding of critical infrastructure and social dynamics. The objectives of the meeting were to

- Identify research areas where STFC and S&T can develop and collaborate on future programs
- Develop joint US-UK research concepts through discussions among researchers
- Publish research concepts in a book to be released by Elsevier in September 2015.

Invitees to this working meeting compromised UK and US researchers from the federal government, national laboratories, universities, and first responders. Invitee backgrounds ranged from cyber infrastructure and cybersecurity to epidemiology and medicine to the social sciences. Infrastructure owners and law enforcement personnel were also included to ensure discussions stayed grounded in mission needs and assumptions were vetted by public safety practitioners. The innovative meeting approach was designed to encourage interactions that would result in research concepts.

This report documents that approach, the presentations and discussions at the meeting, the resulting concept papers, and next steps. Additional detail on the two government agencies, the ColoRS program, the meeting, and participants can be found in the appendixes.

APPROACH: INNOVATION IN MEETING DESIGN

Under the ColoRS program, DHS S&T and STFC sought to bring together a multi-disciplinary and cross-functional scientific community to engage in security research. Securing key experts and speakers to maximize output in a limited amount of time required both extensive pre-planning and a unique meeting structure, as described below.

PRE-EVENT PLANNING

To ensure the ColoRS meeting was effective, the Executive Planning Team engaged in a 12-month process to lay out the scientific and technical challenges, identify and invite the appropriate participants, develop event communications that were timely and clear, and complete all logistical details necessary for a successful meeting. The following flow chart (Figure 1) describes this three-pronged approach to the ColoRS meeting planning and execution. The Executive Planning Team, which was made up of senior leadership from both agencies as well as staff highly conversant in stakeholder involvement, met monthly throughout this 12-month period, with the frequency becoming bi-weekly, and then weekly, as the event approached.

The Executive Planning Team first identified and described three themes that encompassed key challenges in the area of cybersecurity and societal resilience. With support from the Pacific Northwest National Laboratory (PNNL), the team then identified through an iterative process the expertise required to address each theme. The team considered candidates both for the relevance of their specific expertise to the issues being addressed and also that of other possible members of the group, the aim being to create a coherent community of mutually supportive individuals with complementary perspectives. Participants were selected based on their diverse expertise, creativity, and innovative thinking in order to explore and better understand multiple threats and possible responses. The team then invited an appropriate subset to participate in the ColoRS meeting. They also identified appropriate moderators, one from the US and one from the UK, for each theme discussion. In addition, they invited plenary speakers to provide high-level context into the depth of the issues and make a plea to the scientific community to help the US and UK governments address these complex challenges.

As far as the logistical support, the ColoRS working meeting included support to identify a meeting location, secure a hotel room block to contain costs, and develop event information and a registration website that captured key information about each attendee. Communication activities included developing a meeting information packet with invitation signed by a senior representative from the US and UK agencies, detailed agenda, and description of the themes and expectations. The Executive Planning Team, in particular STFC, also worked to identify a reputable scientific publisher that would be interested in releasing a book containing the concept papers following the meeting. STFC also created an online portal for further collaboration among meeting participants. Finally, the Executive Planning Team discussed goals, roles, and responsibilities within the meeting structure with the selected moderators before the meeting to ensure every group would function as designed.

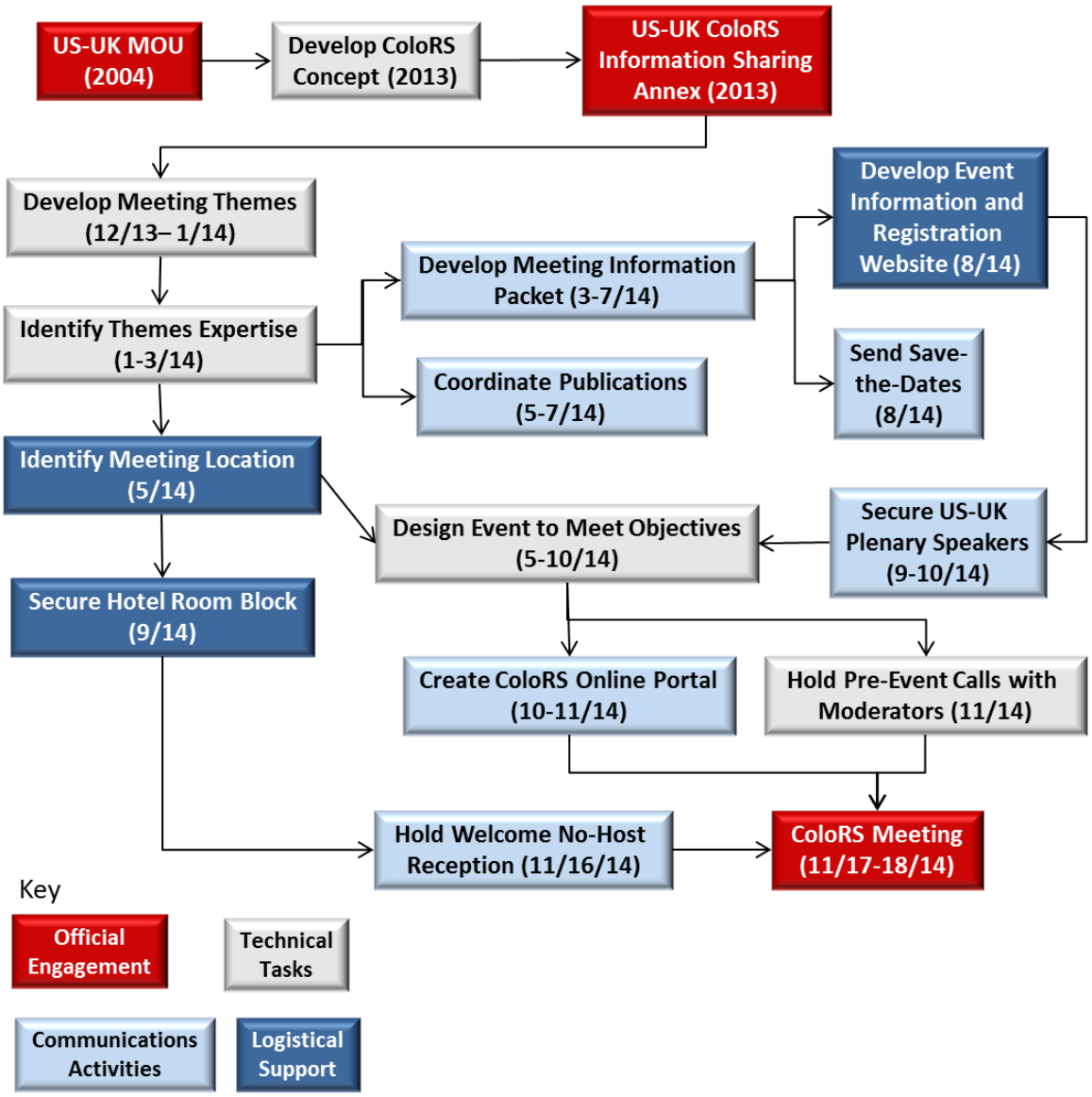


Figure 1 Major Tasks in Developing the ColoRS Working Meeting

MEETING STRUCTURE

The ColoRS meeting was designed to be creative, collaborative, and fast-paced (Figure 2). The Executive Planning Team meticulously considered the structure and agenda of this two-day meeting as they prepared for the event (Figure 3). The meeting began with a no-host reception the night before to help participants become acquainted with each other in preparation for the in-depth discussions planned for the following day.

For the first part of Day 1, plenary speakers from US and UK leadership issued a charge to the group, then meeting participants divided into theme groups where they refined theme descriptions, addressed challenges, and discussed issues and research gaps. Each theme group was provided two moderators, one from the US and one from the UK. Participants were grouped based on their expertise, but were organized to challenge their individual thinking about the problem sets. Emily Saulsgiver acted as over-all meeting facilitator. Quite aside for being a role well suited to her personal strengths, it freed the program leads from the US and UK (Joseph Kielman and Bryan Edwards, respectively) to focus on technical debates within groups, identifying and developing synergies between them.

Toward the end of Day 1, the moderators from each theme provided a summary of discussions within their respective groups, which was captured on flip charts and posters and posted on the walls around each group's section of the room. Participants were then asked to go around the room on a "Gallery Walk" to review the discussions and outputs developed by the others to indicate their interest in various topics and share questions identified by the other groups.

By the end of Day 1, participants prepared initial drafts of research concepts on pre-prepared templates, outlining research questions and concepts that they

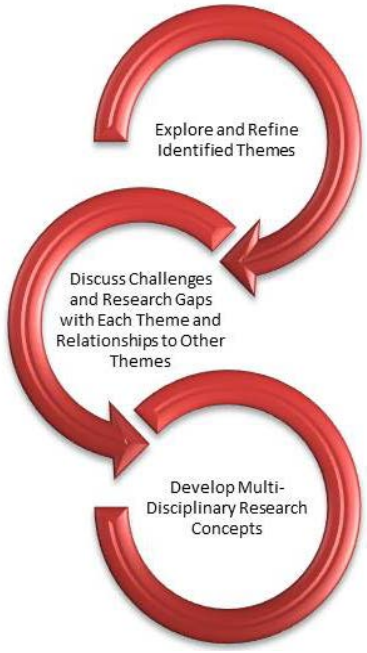


Figure 2 Workshop process

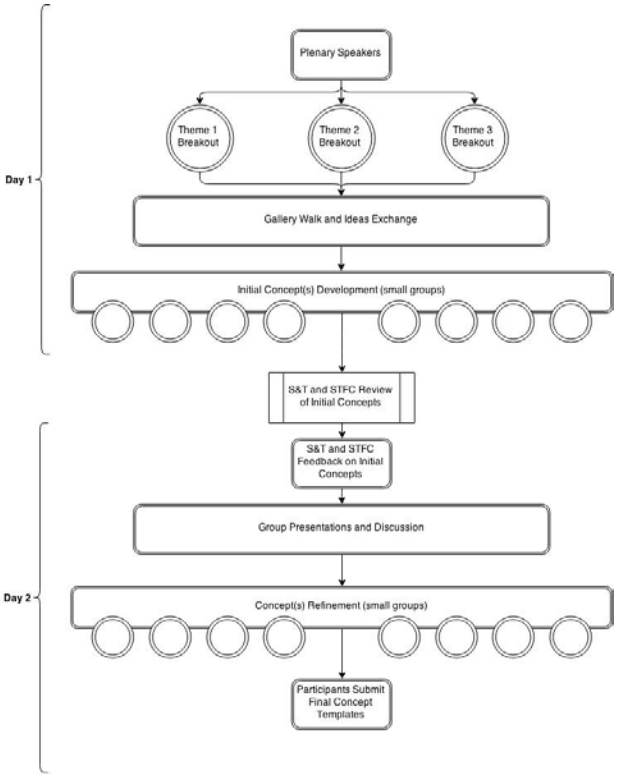


Figure 3 Meeting Structure

were interested in further refining as part of the ColoRS activities. Participants were allowed and encouraged to contribute to multiple concept templates. Participants teamed to complete the templates and develop the research concepts. They were instructed not to work with other participants in their domain in order to explore cross-disciplinary approaches. At the conclusion of Day 1, the S&T and STFC Executive Planning team reviewed the concepts for gaps and duplication.

At the start of Day 2, the Executive Planning Team provided a summary of initial comments on the products of Day 1, followed by additional direction according to the goals and objectives for Day 2. Writing teams presented their concepts to the wider group for input, then revised based on comments. Group discussion was highly productive during this portion of the agenda, with the meeting facilitator capturing the comments, identified gaps, and recommendations on flip charts. This free-flow of discussion enabled concepts to be explored from multiple angles – medical, social science, infrastructure protection, data analysis – and therefore further refined to consider other theories and research requirements to address the challenges. Some concepts were determined to require further decomposition to explore the full extent of the problem. Teams for other concepts added domain expertise from additional research areas to improve investigation into different aspects of the concept. Writing teams further refined the concepts during the afternoon working session, with final versions of the templates collected and logged at the end of Day 2.

Participant Feedback: "Great chance to mix computational science and social science ideas and approaches."

By submitting final versions of the templates, the author(s) committed to expanding each concept into a paper for publication, with the understanding that their concepts would be included in S&T and STFC reports and further discussions related to the event and the two countries' collaboration.

Papers based on these concepts will be included in a book to be released by Elsevier in September 2015. These concepts may also be developed into research proposals for potential joint funding. Beyond these identified outputs, the ColoRS working meeting served to broaden UK and US relationships, establish long-term partnerships among researchers, develop the boundaries of a new research area, start a research roadmap, and encourage researcher exchanges.

"To solve problems associated with cybersecurity, we must stop thinking like researchers and start thinking of ourselves as responders. The key is looking at what we are doing in research and moving it faster into the field."

Dr. Robert Griffin, Deputy Under Secretary, DHS S&T

PLENARY SESSION SPEAKERS: ENCOURAGING A MULTI-DISCIPLINARY PARTNERSHIP

The ColoRS working meeting began with a set of plenary session speakers to set the tone and expectations for the two-day meeting.

DR. DOUGLAS MAUGHAN, DIRECTOR, CYBER SECURITY DIVISION, DHS S&T

This workshop is part of a wider set of bilateral events between the UK and the US meetings this week. The two countries have shared a great partnership from the beginning of DHS and even before with the Department of Defense and the intelligence community. This partnership is especially significant in the cyber security area. Cyber infrastructure is everywhere, making it an area of critical importance. The world is not going back to paper and pencil. But this ability to communicate at the speed of light comes with a cost: We must know how to secure our cyber infrastructure. The working meeting today and tomorrow is aimed at an initial discussion on some important research areas.

DR. ROBERT GRIFFIN, DEPUTY UNDER SECRETARY, DHS S&T

This year marks the tenth anniversary of DHS' longest-lasting bilateral agreement, with the UK. Cyber touches nearly every element of life. The DHS Under Secretary for S&T laid out visionary goals this year, and cyber is a core competency for protecting the homeland. Cyber overlays a number of issues, such as big data and effective screening. It is a necessary component of protecting commerce and balancing privacy, while making first responders safer. To solve problems associated with it, we must stop thinking like researchers and start thinking of ourselves as responders. The key is looking at what we are doing in research and moving it faster into the field. Even more, how can we keep up with the speed at which cyber changes? This is a global problem that will require unparalleled international cooperation. What other partners can we find to deal with cybersecurity holistically? Where are we heading, and how can we strengthen our relationship? These next two days can help address questions like these.

PROF. BERNARD SILVERMAN, CHIEF SCIENTIFIC ADVISOR TO THE HOME OFFICE, UK

The US and the UK are the two leading scientific countries in the world. We have been collaborating for generations and are getting closer over time. The partnership between the two counties is an important one for several reasons. It brings together the two nations' collective experience and knowledge. It allows us to share specialists and techniques and develop much-needed novel solutions. It enables us to unify standards and understand how to use technology in a unified world. We can work together in times of emergencies and prepare more effectively for them. Working together also brings insights and support. In addition, as resources become constrained, cooperation brings efficiencies. Priorities in the Home Office include staying ahead of a diversified threat, responding to unique security challenges, doing as much as we can to challenge extremism and those who practice it, maintaining necessary communications data and lawful intercept capabilities, and continuing to strengthen border and aviation security. We intend to do more to support the security sector. To do so, we must strengthen partnerships with local agencies, public organizations, and private industry. We welcome fresh thinking in this area, because there are clearly breakthroughs to be made. The contacts and relationships started at this meeting will strengthen future work in this area.

PROF. BRYAN EDWARDS, DEFENCE, SECURITY, AND RESILIENCE THEME LEAD, FUTURES PROGRAMME, STFC

The leaders of the research community knew from the outset that something special could be done to improve cybersecurity and societal resiliency if ideas were structured appropriately. Problems cannot be solved by single disciplines alone. We need experts who approach problems in different ways and will work collaboratively with others from different backgrounds. This meeting will be unusual because the breadth of expertise is much broader than in a typical working meeting. In the UK, seven research councils fund academic research through money from the government. STFC does this too, but in addition operates UK National Laboratories and manages the UK's participation in large infrastructure-dependent science projects overseas (e.g., CERN). What people often remember is our work in particle physics and astronomy, but a substantial part of the research we undertake or support is in other areas (e.g., advanced high-performance computing).

DR. JOSEPH KIELMAN, SENIOR SCIENTIFIC ADVISOR, CYBER SECURITY DIVISION, DHS S&T

One of the drivers for ColoRS is to look at how cybersecurity is attached to societal resilience. This view requires research beyond new technologies. The complex interplay between technical, social, ethical, political, policy, and economic considerations is often self-evident. Challenges involve the protection of citizens, protection of the critical infrastructure on which normal functioning of society depends, and the resilience of that society to a wide and rapidly evolving series of natural and human-made threats. ColoRS will expand relationships and allow us to explore these challenges in a multi-disciplinary and fundamentally new way. It is our hope that jointly funded projects will be formed as a result of the relationships made and the outputs of the next two days.

"The leaders of the research community knew from the outset that something special could be done to improve cybersecurity and societal resiliency if ideas were structured appropriately. Problems cannot be solved by single disciplines alone. We need experts who approach problems in different ways and work collaboratively with others from different backgrounds."

Prof. Bryan Edwards, Defence, Security, and Resilience Theme Lead, Futures Programme, STFC

COLORS THEMES: HOW DOES CYBERSECURITY RELATE TO SOCIETAL RESILIENCE?

To start discussion and brainstorming activities, participants were organized into three groups to address three themes engrained in the relationship between a society's resilience, its reliance on cyber infrastructure, and the absence of vulnerabilities and disruptions that impact civilian livelihood and safety.

THEME 1: SECURING INFRASTRUCTURE FROM CYBER DISRUPTIONS

There is little doubt that advances in computing (both hardware and software), sensor technology, and telecommunications have had a profound effect on how we lead our lives. For many citizens, these changes have brought great benefits. The innovations have also permeated our critical infrastructures and radically changed how they operate. So widespread, and deeply embedded, have the innovations become that individuals, societies, and the commercial world all risk becoming blind to the extent to which they have crossed the line between convenience and dependence on the new pervasive cyber infrastructure. We assume our cyber infrastructure will serve us well under all circumstances; however, how right are we in this assumption?

This theme considered the nature of the risks posed by society's dependence on cyber technology and specifically the underlying critical infrastructures on which services depend. It considered both tangible (e.g., hardware) and intangible (e.g., data) elements and sought to determine previously unidentified vulnerabilities and how they could be addressed. The discussion came primarily from a computer sciences perspective.

US Participants	UK Participants
• Joe Jarzombek, DHS National Protection and Programs Directorate (Facilitator) • Dennis Egan, Rutgers University • Peter Freeman, Georgia Institute of Technology • William Streilein, Massachusetts Institute of Technology (MIT) Lincoln Laboratory	• Sadie Creese, University of Oxford (Facilitator) • David Hutchinson, University of Lancaster • Andy Marshall, Rhead Group

KEY QUESTIONS SURROUNDING THEME 1

- What clouds/networks exist that support critical infrastructure?
- What are the security and failure risks associated with the cloud?
- Of the many critical infrastructure categories that exist, which are the high cloud users and what specific risks are associated with them?
- What recovery strategies will allow us to protect critical infrastructure? How can we prevent attacks?

- What do we know about the infrastructure data: what it is, how is it structured?
- What do we know about the sharing process? Who needs which parts? How can we build a framework to facilitate sharing?
- How can we understand attacks at the infrastructure and enterprise level? Are attacks cascading? Can we be predictive?
- What outcomes do we want at the end, recovery to a greater resilience?
- Who leads processes at the local and national level? Who "owns" the risk? How does this impact the system?
- What role should adaptation and training play?
- What role do exercises play? What constitutes an effective cybersecurity exercise?

THEME 1 DISCUSSION

Discussions centered around the interdependencies of components, societal and individual behaviors in relationship to technology systems, the roles of government versus private industry, and varying information needs. Appendix F contains additional details on the discussion.

Creating resiliency must involve monitoring and metrics, technology and people, situational awareness and operations. Both the UK and the US have lists of key infrastructure binned by critical infrastructure sector. We lack a comprehensive model and framework to predict ripple/cascading effects among complex interdependencies. How might the infrastructure evolve? At what scale must we understand risk exposure–individually, nationally, globally? What about the supply chains? What comprises the system, its assets, and its brand? How will its failure affect markets? The integrity of the building blocks does matter.

Participant Feedback: "Fantastic interaction with people from different disciplines. Opportunities to work with people I'd rarely have engagement."

Equally important are the roles, responsibilities, and behavior of individuals in organizations in relationship to technology systems. Accountability must lead to action. We also need to consider societal response to support decision-making.

Another challenge is ownership, which might be government or private industry, perhaps even foreign entities. Industry normally prefers to address its own problems with no help from government, but industry, particularly smaller companies, may not have the internal capabilities to understand or address cybersecurity. Even if the government provided information that a threat had been detected, some companies may not want to know that their systems are vulnerable because then they would be

obligated to act. Can we supply incentives–to the companies to build more resilient system, to the suppliers to deliver more resilient products? We need to connect the infrastructure and the mission.

The challenge for communication is the speed at which the event will happen. What information does the infrastructure owner have? What do the operators need? What does the responder need? What does the community need? The three most important factors are the time, the quality of the information, and the destination of the information. Social media represents both an opportunity and a challenge.

THEME 2: MODELING AND MEASURING SOCIETAL RESILIENCE

Should the cyber infrastructure on which society is now increasingly dependent be degraded or lost, either locally or nationally and whether by natural disaster or deliberate interference, the effects will be profound. Some failures, such as loss of power or health services, may be felt immediately. Others, such as food and fuel shortages resulting from the failure of just-in-time logistics systems, may take longer to manifest themselves. Other failures may occur as a result of currently unrecognized and/or poorly understood interdependencies that could become apparent only some time or some distance after the initial failure.

This theme sought to better understand the possible short- and longer-term effects of a cyber-related event on social structures. It clarified what we mean by resilience and identified analytical methods, approaches, and metrics that could be used to measure it. The discussion came from a computational social sciences perspective.

US Participants	UK Participants
• Thomas Sharkey, Rennselaer Polytechnic Institute (Facilitator) • Nina Fefferman, Rutgers University • Kevin Keenan, College of Charleston • Alexander Siedschlag, The Pennsylvania State University	• Jennifer Cole, Royal United Services Institute for Defence and Security Studies (Facilitator) • Jon Coafee, University of Warwick • Catherine Hemmings, Thames Valley Police • Malcom Sperrin, Royal Berkshire Hospital • James Sterbenz, University of Kansas and University of Lancaster • Pete Fussey, University of Essex

KEY QUESTIONS SURROUNDING THEME 2

- What are plausible cyber failures?
- What are the tiers of resilience? What constitutes recovery in the short- and long-term?
- How can we model individual and societal responses to cyber failures?
- How do people interact and react under various stress conditions?
- What are the interdependencies of infrastructure protection and societal practices?

- At what point does the system break down?
- What can we measure and use as indicators?
- How do we detect or understand an attack without knowing what "normal" is?

THEME 2 DISCUSSION

Discussions ranged from changes in leadership and governance to the effect on different segments of society and the need for common terminology on the issues. Appendix F contains additional details on the discussion.

Different segments of society are likely to feel different impacts. For example, the Amish may feel minimal effects from a cyber-disruption. How do the law-abiding and non-law-abiding players respond differentially to events? It has been said that the "normal" condition of the network is to be under constant attack, but the concept of "normal" is not universal and might be defined by smaller groups at a local level. How does a large entity restore one "normal" to all?

Another area to consider will be leadership and governance. Whoever governs must have credibility and legitimacy, and different social groups have different leaders with those traits. Do we really understand how dependent we are on cyber systems? Could we revert to doing complex situations without a cyber-system, or has society fundamentally changed? How would local governments cope failing knowledge from higher up?

Participant Feedback: "Great international-ism – adds an excellent dimension to research"

Another issue will be the ability to communicate in common terms. We must define the aspects of resilience to know where we can agree and disagree and facilitate coming together in overlapping areas of interest and concern. It may be that we need categories of function rather than categories of failure. For instance, losing the ability to go to work if the Internet is down cuts across multiple types of workplaces. Would it be wise to force the Internet to cache and operate locally, reducing reliance on overall, widespread connectivity? We would be reducing the reliance on global connectivity to maintain local function.

THEME 3: ANALYTICS FOR EFFECTIVE DATA EXPLOITATION

By its very nature, cyber and sensor infrastructure is becoming increasingly pervasive, giving rise to vast amounts of diverse data moving across high-speed networks and processing centers and stored in large and diverse databases across a range of public and private sector organizations. Whether it is to exploit

the latent potential of the information stored in this data, or to monitor the health and performance of infrastructure for early signs of potential failure or attack, advanced real-time data and visual analytics will be required.

This technical theme considered where continuous aggregation of streaming and batch analytics could be improved and better utilized for homeland security. For such applications, current shortfalls such as system resilience and response, issues with privacy, and both the government's and society's willingness to share information were also discussed.

US Participants	UK Participants
• Steve Stein, PNNL (Facilitator) • Eduard Hovy, Carnegie Mellon University • Vladimir Kolesnikov, Bell Labs • Mark Greaves, PNNL	• Erica Yang, STFC (Facilitator) • Min Chen, University of Oxford • Theresa Chambers, UK Government, Home Office

KEY QUESTIONS SURROUNDING THEME 3

- How can we create and improve models rapidly for those who monitor?
- How do we evaluate the effectiveness of the model?
- To what extent does information sharing benefit society? How do models and policies about information sharing affect resilience?
- How do we design command and control systems that take into account human interactions, cyber infrastructure, uncertain information, distributed systems, uneven education, and other complexities?
- What are the right principles on which to base executable flexible policies to allow humans to respond to Black Swan events?
- What negative and positive lessons can we learn from biological systems?
- How can we consider the scale issues surrounding machine learning and data sanitization?
- What is the range of responses, and when do we take specific actions? What are the thresholds? In the absence of specific knowledge or cause, how do we describe appropriate response options?
- In an emergency, what resources and information are shared? What are the legal implications of who is allowed to see what in an emergency? In a cyber-world, what is the boundary to protect personal privacy when society is facing major threats?
- What is normal? What are the characteristics of normal? How do we measure them?

THEME 3 DISCUSSION

Discussions focused on the data, analysis, and models needed to identify and respond to cyber anomalies as well as the needs of data owners and the manner in which humans respond. Appendix F contains additional details on the discussion.

While the goal may be streaming data—as real-time as possible—the reality is that data are generated in an unorganized manner and only occasionally in tabular form and time stamped. Analytical models applied to such raw data can only generate warnings or prioritized information. Because of complexity, we cannot look for failures in signatures. Instead, we look for patterns that are suggestive of failure, probabilistic of failure. If we see a pattern that has no precedence, that pattern could be examined and added to the database so that correlations grow with time. If something triggers a warning, then we need to be able to go back and mine the data to determine what is happening. We can also look at the growth of abnormalities. If the rate is really fast, we must shut down everything and focus on the problem. But, what if we cannot shut everything down? Early recognition, emergency monitoring, and then appropriate response are key. Historical analysis can be undertaken when we have the luxury of time. We are looking at slow, methodical, and smart opponents. If we always monitor the same things, our success at identifying attacks will be low. Because we cannot move quickly enough to isolate the cause, we take Draconian action. If we could rapidly find the cause, we could react more appropriately.

How can we utilize private data that is rarely if ever seen by government agencies? How can we erect barriers between organizations that enable information sharing with adequate protection? Policy can constrain the types of questions that can be asked of the data. A database protected by cryptography can be set up with levels of authority, and some users can access deeper.

Participant Feedback: "This is the place where big ideas come out."

We must examine the human side of the equation, considering three categories of actors:

1. Operators for monitoring, heavily assisted by automated methods. They deal with streaming data.
2. Analysts, who look into special cases and use historical data, are more skilled and knowledgeable.
3. Modelers, who check to make sure our decision processes and models still work, create new models, and identify new data sources. They train the other two categories.

What tools and skills does each category need?

"The complex interplay between technical, social, ethical, political, policy, and economic considerations is often self-evident in cybersecurity. Challenges involved the protection of citizens, protection of critical infrastructure on which normal functioning of society depends, and the resilience of that society to a wide and rapidly evolving series of natural and human-made threats."

Dr. Joseph Kielman, Senior Scientific Advisor, CSD, DHS S&T

RESULTS: NEW CONCEPTS FOR CYBERSECURITY CONSIDERING SOCIETAL RESILIENCE

Ten initial concept papers at the end of Day 1 grew out of theme discussions with interactions from other participants during the "Gallery Walk." These concepts were then thoroughly reviewed by the all participants through in-depth discussion and brainstorming on Day 2. The writing teams further refined their concepts in small groups by the end of Day 2. The results consisted of 19 multi-disciplinary concepts. The progression of the initial concepts to the final results is shown in the table below, with the full description of each final concept in the following theme sections.

The Information Sharing Annex supporting the ColoRS activities outlined its objective of developing a joint approach to increase engagement between the US and the UK research communities. The results of the ColoRS meeting achieved this objective by demonstrating a new process by which the two countries may collaborate when determining areas of mutual research interest. In addition, the meeting enabled relationships to form among researchers from the US and UK, with immediate results seen through the publication of the meeting information in *Crisis Response Journal* and with Nina Fefferman of Rutgers University being provided access to STFC facilities directly following the meeting conclusion. These relationships are expected to reap additional rewards in the future, including through the publication of a book containing the fully developed research concepts.

ColoRS Meeting Concept Progression from Day 1 to Day 2

Theme: Securing Infrastructure from Cyber Disruptions

Day 1 Concept (Initial)		Day 2 Concept (Refined)
1. Situational Awareness for Resilient Cyber Infrastructures	→	1. Co-Evolution of Resilient Enterprises Together with a Cybersecurity Command and Control Center 2. Functional Cyber Situational Awareness 3. Collecting and Sharing Sufficient Information to Understand and Mitigate Risk Exposure
2. Architecture and Design for Resilient Systems	→	4. The Human Element in Resilient Systems Design 5. Architecture and Design for Resilient Cyber Systems 6. Network Architecture for Resilience-Enabling Micronets
3. Understanding the Unique Aspects of the Restoration/ Recovery of Infrastructure and Social Networks from Cyber-Related Attacks	→	7. Multi-Agency Response Structure to Cyber-Attack 8. Understanding the Unique Aspects of the Restoration/Recovery of Infrastructure and Social Networks from Cyber-Related Attacks

Theme: Modeling and Measuring Securing Infrastructure from Cyber Disruptions Societal Resilience

Day 1 Concept (Initial)		Day 2 Concept (Refined)
4. Cyber-Threats and the Perception of a Dependent Society	→	9. Cyber-Threats and the Perceptions of a Dependent Society 10. Micronet-Enabled Resilient Societies: US-UK Comparison
5. Dynamic Topologies of Responsibilities and Governance in a Cyber-Disabled Era	→	11. Dynamic Topologies of Responsibilities and Governance in a Cyber-Disabled Era
6. Resilient Infrastructure and Society That Remains Operable When Cut-Off/in Isolation	→	12. Cyber Threats in the Context of a Challenged and Changing World Order 13. Threat Analysis

Theme: Streaming Analytics for Effective Data Exploitation

Day 1 Concept (Initial)		Day 2 Concept (Refined)
7. Cyber Decision-Making in the Presence of Noisy, Voluminous Data, Using Gold Standard Analogies	→	14. Cyber Decision-Making in the Presence of Noisy, Voluminous Data, Using Gold Standard Analogies
8. Privacy-Preserving Information Sharing	→	15. Privacy-Preserving Information Sharing 16. Privacy, Policy, and Public Perception (Are we preserving the wrong privacy?)
9. How Do You Rapidly Develop and Improve Models in Streaming Analytics?	→	17. How Do You Rapidly Develop and Improve Models in Streaming Analytics?
10. Modeling, Monitoring, and Recognizing Potentially Dangerous Changes to Cyber Situations	→	18. Modeling, Monitoring, and Recognizing Potentially Dangerous Changes to Cyber Situations 19. Cascading Impacts: Multi-Dimensional Analysis of Infrastructural, Societal, and Vulnerability Networks

THEME 1: SECURING INFRASTRUCTURE FROM CYBER DISRUPTIONS

The following final concept papers grew out of the discussion on Theme 1 and contributions from all meeting participants:

Co-Evolution of Resilient Enterprises Together with a Cybersecurity Command and Control Center

Team: David Hutchison (University of Lancaster) and Min Chen (University of Oxford)

Interconnections form the backbone of resilient systems. How would we build a command and control system that would observe, report, and control emergencies? The approach will be built around a case study.

Functional Cyber Situational Awareness

Team: William Streilein (MIT Lincoln Labs), Sadie Creese (University of Oxford), Dennis Egan (Rutgers University)

A new approach to situational awareness is needed for social resilience. Cybersecurity quality and resiliency are inherently redundant, with many ways to achieve a function. The approach will develop a model to define data points that allow us to see equivalencies and the data streams that would allow us to maintain them. The results will build a picture of current achievements in functionality and predict function in cyber events. From there, we can reason about the characteristics of function and identify places that need to be bolstered as well as those critical to response.

Collecting and Sharing Sufficient Information to Understand and Mitigate Risk Exposure

Team: Joe Jarzombek (DHS NPPD) and Dennis Egan (Rutgers University)

The work will seek to understand and exploit potential of components (architecture, design, software, hardware, networks, and communications) and processes/behaviors that expose cyber infrastructure to risk. It will also focus on understanding and enhancing means for information sharing in a timely manner to better mitigate risks.

The Human Element in Resilient System Design

Team: David Hutchison (University of Lancaster), James Sterbenz (University of Kansas/University of Lancaster)

The design and operations of resilient systems and services for critical infrastructure must take into account the human element (for example, roles, responsibilities, behavior). People are a critical component of any information technology system that provides or supports critical infrastructure and services. We often compare performance of software and other components. We need to do the same with the human component.

Architecture and Design for Resilient Cyber Systems

Team: David Hutchison (University of Lancaster)

New architectures and designs of resilient networked systems are needed to support critical services and infrastructures. The arguments have previously been well rehearsed, but much remains to be done, not least to demonstrate the feasibility of building such systems. This work will focus on two elements of resilient enterprises: 1. Co-evolution of resilient enterprises together with a cyber-security command and control center, and 2. The human element in resilient systems design.

Network Architecture for Resilience-Enabling Micronets

Team: Thomas Sharkey (Rensselaer Polytechnic Institute), James Sterbenz (The University of Kansas/University of Lancaster), Jennifer Cole (Royal United Services Institute for Defence and Security Studies), and Kevin Keenan (College of Charleston)

This feasibility study will examine the technology aspects of a self-contained micronet that could operate independently or connect to wider networks. What sort of physical protection and resources would be needed? Where would we locate the components and who would own them?

Multi-Agency Response Structure to Cyber-Attack

Team: Andy Marshall (Rhead Group), Steve Stein (PNNL), Dennis Egan (Rutgers University), and Ann Lesperance (PNNL)

How can we team most effectively under a cyber-attack? The approach will examine the information exchange between three main actors in the US and UK: critical infrastructure providers, responders, and the community including local businesses. The work will look at where information is held and what can be shared, at the appropriate quality, and in the appropriate time and place. Research will also look at command and control within the interagency structure and the how and why of consequence management.

Understanding the Unique Aspects of the Restoration/Recovery of Infrastructure and Social Networks from Cyber-Related Attacks

Team: Thomas Sharkey (Rensselaer Polytechnic Institute)

What does cyber restoration and recovery mean? This work will better compare and contrast the recovery strategies necessary for a cyber-attack as opposed to a natural disaster. The results will aid in the development of models for cyber disruptions.

THEME 2: MODELING AND MEASURING SOCIETAL RESISLENCE

The following final concept papers grew out of the discussion on Theme 2 and contributions from all meeting participants:

Cyber Threats and Perceptions of a Dependent Society

Team: Malcom Sperrin (Royal Berkshire Hospital) and Alexander Siedschlag (The Pennsylvania State University)

This research will make the business case for cybersecurity. We need to contextualize concepts to inform operations for a loss of cyber networks and what effects that could have so that people can understand their vulnerability. An analog exists in a hospital in a war zone. There is no cyber network, yet the ability to provide medical care is not compromised and may be enhanced. We must be able to embed social perceptions into operational demands and translate breeches into mission/business impact. Many in society think of a cyber-attack as something that might hit their individual fire walls and be fought off by virus protection. Data might be compromised, but all will be well in a short time. We need to look at things like the availability of acceptable data, how cyber impacts on social structures, consequences of attack, and barriers to credibility. The approach will be to build a bridge between academic components and how we get individuals and organizations to respond more appropriately.

Micronet-Enabled Resilient Societies: UK-US Comparison

Team: Jennifer Cole (Royal United Services Institute for Defence and Security Studies), Kevin Keenan (College of Charleston), Thomas Sharkey (Rensselaer Polytechnic Institute), and James Sterbenz (The University of Kansas/ University of Lancaster)

Using US and UK case studies of major outages and disasters, this research will examine the extent to which communities/individuals are dependent and perceive themselves to be dependent on the networks, systems, and data. How are functions degraded when these systems and networks are ravaged? Which resilience measures might be prepared and enacted? To what extent are vulnerabilities understood and how do they differ depending on context? What is actually needed?

Dynamic Topologies of Responsibilities and Governance in a Cyber-Disabled Era

Team: Peter Freeman (Georgia Institute of Technology), Jon Coaffee (University of Warwick), Nina Fefferman (Rutgers University), and Kevin Keenan (College of Charleston)

The focus is on who has the influence during cyber disruption. Whose responsibility is it to restart the system, and who has the ability to resolve the issue? Scale isn't something fixed. Command and control is somewhat fixed, but people inhabit lots of scales at the same time, with varying amounts of self-organization. There will be gatekeepers of isolated nets with legitimacy in different communities. How does informal governance occur? Are there optimal forms? How can we enable the flow and velocity of communications? How can we embed that knowledge into policy for efficiency? The results will be more optimized and resilient systems against cyber-attack. The approach will be to mathematically model relationships and bonds between people and how these relationships change based on events.

Cyber Threats in the Context of a Challenged and Changing World Order

Team: Malcom Sperrin (Royal Berkshire Hospital)

Emerging countries present threats and opportunities. A subtlety is rising of new expectations and standards, particularly with overlapping US and UK approaches. Acceptable behavior differs from current practice. The approach will be to look at state-sponsored cyber challenges and the new "best practices" and end products.

Threat Analysis

Team: Malcom Sperrin (Royal Berkshire Hospital)

How can we build a chain of events, with probabilities, for a cyber-attack? What are the relevant constraints? This paper will address such questions and provide an analysis of key indicators.

THEME 3: STREAMING ANALYTICS FOR EFFECTIVE DATA EXPLOITATION

The following final concept papers grew out of the discussion on Theme 3 and contributions from all participants:

Cyber Decision-Making in the Presence of Noisy, Voluminous Data, Using Gold Standard Analogies

Team: William Streilein (MIT Lincoln Laboratory), Malcom Sperrin (Royal Berkshire Hospital), and Dennis Egan (Rutgers University)

Other sectors have promulgated "gold standard" descriptions of data in certain situations such as disease spread and programming languages. These standards ensure that the data is true for the intended claim. Can we apply such standards to cyber data? The research will look for analogous approaches and how they might work in a cybersecurity methodology, including developing datasets to test such a methodology for the integrity of the data and its process.

Privacy-Preserving Information Sharing

Team: Vladimir Kolesnikov (Bell Labs)

Agencies and private companies struggle to trust each other enough to share information that could be critical to detecting, preventing, and responding to a cyber-attack. "Big Data" is not sitting in one place, within one organization; its potential cannot be realized without a way to share information. Cryptography can be used to enable information sharing through secure communications. The approach will examine processes developed at Bell Labs against a case study.

Privacy, Policy, and Public Perception

Team: Nina Fefferman (Rutgers University) and Cat Hemmings (Thames Valley Police)

Many cyber security activities are hindered by a lack of clarity on what "privacy" means. The public doesn't have the vocabulary to express concerns regarding risks, security, and needs. This research will look at both the theory and policy surrounding the term, examining how privacy is used in various frameworks and the rights to privacy and why they were created. The results should help explain concerns of privacy to the public and help determine the types of information that should be made public.

How Do You Rapidly Develop and Improve Models in Streaming Analytics?

Team: Mark Greaves (PNNL), Min Chen (University of Oxford), and Theresa Chambers (UK Home Office)

Streaming analytics pours millions of bits of data that must be accounted for in system models that help monitor performance and pinpoint threats. Traditional approaches may not work in this dynamic environment. Can we use visualization techniques to design and improve models more quickly? The approach will look at the potential for an integrated command and control structure.

Modeling, Monitoring, and Recognizing Potentially Dangerous Changes to Cyber Situations

Team: Eduard Hovy (Carnegie Mellon University), Erica Yang (STFC), and Mark Greaves (PNNL)

Multifaceted knowledge is embedded in analytics and models. What characterizes the data? How can we evolve models using realistic data that allows us to identify normal versus abnormal and easily warn of changes? How can we utilize the connections between data and society to identify cascading impacts or vulnerabilities we might not have seen before? This feasibility study will help answer such questions.

Cascading Impacts: Multi-Dimensional Analysis of Infrastructural, Societal, and Vulnerability Networks

Team: Pete Fussey (University of Essex), Nina Fefferman (Rutgers University), Jon Coaffee (University of Warwick), and Cat Hemmings (Thames Valley Police) (crosses Themes 2 and 3)

Cyber infrastructures are embedded into different infrastructures as well as social groups. This research will deploy mathematical-weighted multi-graphs in tandem with social science/sociological insights to integrate cascading impacts of cyber disruption. The work will identify and assess the diverse impacts of cyber disruptions on 1) other infrastructures, 2) social settings, and 3) forms of vulnerability. This effort will also help reveal interrelationships and interdependencies.

"ColoRS has the potential to not only change how we solve cybersecurity challenges but to change the way we approach research and development partnerships."

Emily Saulsgiver, Meeting Facilitator and Member of the Executive Planning Team, Contracted Support to DHS S&T

NEXT STEPS: TOWARD A MORE RESILIENT CYBER COMMUNITY

Following the success of the ColoRS meeting, the following steps will be taken to enhance the partnership and the research collaboration of the attendees and advance US-UK collaborations in resilience and security.

DEVELOP COLLABORATIVE RESEARCH PAPERS/BOOK FOR PUBLICATION

As was highlighted throughout the ColoRS meeting, the concept papers and ideas that were developed as a part of the discussions will serve as key chapters of a comprehensive book that will be published in the by Elsevier in September 2015 (targeted date). Meeting participants have agreed to work to the timeline illustrated in Figure 4 to meet Elsevier's publication deadlines.

DEVELOP OUTREACH AND COMMUNICATION STRATEGY

Gaining visibility and awareness of the research and products that are developed as part of the ColoRS program will be important to ensure that the value of this collaboration is shared with broader audiences to inform future engagements. ColoRS will provide valuable input on how to enhance US-UK research from a multi-disciplinary or end-user perspective. One approach will be to share ColoRS updates with participants and internal and external interested audiences. The program updates will highlight key activities, results, and upcoming meetings and conferences may be of interest. The outreach and communication strategy to be developed will target some of the following audiences:

- **The two key national-level sponsors of the ColoRS program, namely DHS S&T and STFC**. This internal outreach will ensure partners and other program officers within these organizations are aware of the results of the ColoRS program. Ideally, staff within these organizations will continue to support the results and next steps of ColoRS.
- **Other research agencies across the US and UK**. These external engagements by DHS S&T, STFC, and their contracted support teams will ensure awareness of the ColoRS activities and goals through the broader research community. Outreach targets consist of other federal research organizations, academic institutions, national laboratories, the private sector, and homeland security stakeholders.

- **The broader homeland security community**. ColoRS results will be highlighted at appropriate conferences and meetings for further input and engagement. DHS S&T and STFC will work within their organizations to identify potential speaking events where ColoRS might be highlighted.
- **Other international partners with which DHS S&T and STFC have relationships**. DHS S&T and STFC will work through their organizations to engage other partners to highlight ColoRS and vet the approach and outcomes.

Regular communications with participants and interested parties will be crucial to the future success of the ColoRS program. Thus, S&T and STFC will jointly prepare regular communications materials (e.g., a quarterly newsletter sent via email) to ensure transparency and awareness of all ColoRS-related activities.

DEVELOP COLORS OUT-YEAR STRATEGY FOR DHS S&T AND STFC

DHS S&T and STFC will collectively develop a strategy document to outline both the objectives of the engagement and methods to achieve them. The strategy document will lay out a process for a US-UK collaborative approach to identify joint research challenges and topics of mutual concern, along with collaboratively funded research projects. Questions to guide the development of this strategy include the following:

- What do S&T and STFC hope to achieve from the collaboration?
- Why is this collaboration important?
- What will happen as a result of the collaboration?
- Where are we now?
- How can we achieve results?
- What are the guiding principles?
- How will we judge the quality of our results?

As a part of this activity, S&T and STFC will look for opportunities to leverage with other programs to

- Develop new themes for potential collaboration
- Explore other activities and approaches to enhance the ColoRS partnership
- Develop collaborative research and development programs and exchanges
- Develop an international strategy engagement for ColoRS.

BEGIN PLANNING THE COLORS WORKING MEETING FOR 2015

S&T and STFC gained significant insight through the planning and execution of the 2014 ColoRS meeting and process. S&T and STFC would like to duplicate this process and outcomes of the collaboration as quickly as possible to keep momentum and demonstrate value to the end-users of this research. The ultimate goal is to build a bridge that enables continual engagement and value to the broader homeland security community in the US and UK. To accomplish this, S&T and STFC will immediately begin to identify the themes and objective for the next ColoRS meeting, to be held in the fall of 2015 in the UK.

The Executive Planning Team would like to thank all participants for making the first ColoRS working meeting a success and giving so generously of their time, insights, and expertise to help solve challenges in cyber security and societal resilience.

APPENDIX A: AGENCY SPONSORS

US DEPARTMENT OF HOMELAND SECURITY SCIENCE AND TECHNOLOGY DIRECTORATE

Technology and threats evolve rapidly in today's ever-changing environment. The Science and Technology Directorate (S&T) of the Department of Homeland Security (DHS) monitors those threats and capitalizes on technological advancements, developing solutions and bridging capability gaps at a pace that mirrors the speed of life. S&T's mission is to help strengthen America's security and resiliency by providing assessments, analysis, and reports and developing innovative technology solutions for the homeland security enterprise.

Created by Congress in 2003, DHS S&T conducts basic and applied research, development, demonstration, testing, and evaluation activities relevant to homeland security. DHS S&T strives to address current capability gaps while preparing for future challenges. Projects are organized into six primary areas that directly support DHS components, as well as federal, state, and local first responders:

- **First responders**: expanding capabilities and improving effectiveness, efficiency, and safety
- **Borders and maritime security**: enhancing security at the nation's borders and waterways without impeding the flow of commerce.
- **Cybersecurity**: contributing to a safe, secure, and resilient cyber environment
- **Chemical and biological defense**: detecting, protecting against, responding to, and recovering from chemical and biological incidents
- **Resilience**: improving the nation's preparedness for natural and human-made catastrophes.

In particular, the Cyber Security Division's mission is to contribute to enhancing the security and resilience of the nation's critical information infrastructure and the Internet by

1. Developing and delivering new technologies, tools, and techniques to enable DHS and the US to defend, mitigate, and secure current and future systems, networks, and infrastructure against cyber-attacks
2. Conducting and supporting technology transition
3. Leading and coordinating research and development among the scientific and engineering community that includes department customers, government agencies, the private sector, and international partners.

UK SCIENCE AND TECHNOLOGY FACILITIES COUNCIL

The Science and Technology Facilities Council (STFC) is one of the UK's seven publicly funded research councils responsible for supporting, coordinating, and promoting research, innovation, and skills development in seven distinct fields. The council's breadth of science and the sheer diversity of its

portfolio allows it to harness world-leading expertise, facilities, and resources to drive science and technology forward and maximize its impact for the benefit of the UK and its people.

STFC research delivers a non-stop flow of fundamental insights and breakthroughs in spheres ranging from particle and nuclear physics to space, laser, and materials science, meeting real-world requirements through new medicines, cleaner energy, safer aircraft, pioneering security solutions, and much more. Through its UK operations and involvement in major international collaborations, the results of the research through STFC generate outcomes that shape societies, strengthen economies, build industries, create jobs, and transform lives.

In particular, the Futures Programme is working to broaden the impact of STFC's science and technology into areas that are strategically important to the UK. The main focus is on global challenge areas in energy, the environment, healthcare, and security. The Futures Programme is also engaged across government in helping address the policies and programs of UK government departments with responsibility in these areas, engaging policy makers, horizon scanning for relevant science and technology trends, and stimulating activities aimed at addressing government needs.

APPENDIX B: LIST OF ATTENDEES

Theresa Chambers
Head of Profession for Operational Research
UK Government, Home Office

Min Chen
Professor, Visualization and Visual Analytics
University of Oxford

Jon Coaffee
Professor, Security and Urban Resilience
University of Warwick

Jennifer Cole
Senior Research Fellow, Resilience and Emergency Management
Royal United Services Institute for Defence and Security Studies

Sadie Creese
Professor, Cybersecurity
University of Oxford

Jeffrey Dewhurst
Support Contractor
Cyber Security Division, DHS Science and Technology Directorate

Bryan Edwards
Defence, Security, and Resilience Programme Leader
UK Science and Technology Facilities Council

Dennis Egan
Research Professor
Command, Control and Interoperability Center for Advanced Data Analysis, Rutgers University

Linda Enderby
Stakeholder Management
UK Science and Technology Facilities Council

Nina Fefferman
Associate Professor, Mathematics of Complex Systems
Command, Control and Interoperability Center for Advanced Data Analysis, Rutgers University

Peter Freeman
Emeritus Dean and Professor, Future of the Internet and Computing
Georgia Institute of Technology

Pete Fussey
Professor, Resilience, Surveillance, and Society
University of Essex

Mark Greaves
Technical Director, Analytics
National Security Directorate, Pacific Northwest National Laboratory

Robert Griffin
Deputy Under Secretary
DHS Science and Technology Directorate

Catherine Hemmings
Senior Intelligence Analyst
Thames Valley Police, UK

Eduard Hovy
Professor, Computer Science and Natural Language Processing
Carnegie Mellon University

David Hutchison
Professor, Computer Networks, Future Internet, and Resilience
University of Lancaster

Joe Jarzombeck
Director, Software and Supply Chain Assurance
Office of Cyber Security and Communications
DHS National Protection and Programs

Kevin Keenan
Assistant Professor, Research on Awareness of Vulnerabilities to Terrorism
University of Charleston

Joseph Kielman
Senior Science Advisor
Cyber Security Division, DHS Science and Technology Directorate

Vladimir Kolesnikov
Technical Staff, Secure Computation, Privacy, and Security
Bell Labs

Regina Lundgren
Strategic Consultant
Support to the Pacific Northwest National Laboratory

Andy Marshall
Principal Consultant – Resilience
Rhead Group

Douglas Maughan
Director, Cyber Security Division
DHS Science and Technology Directorate

Jessica Sandusky
Research Scientist
Pacific Northwest National Laboratory

Emily Saulsgiver
Program Coordinator
Cyber Security Division and Office of University Programs, DHS Science and Technology Directorate

Thomas Sharkey
Assistant Professor, Operations Research, Network Restoration
Rensselaer Polytechnic Institute

Alexander Siedschlag
Professor and Chair of Homeland Security
The Pennsylvania State University

Bernard Silverman
Chief Scientific Advisor
UK Government, Home Office

Malcom Sperrin
Director of Medical Physics
Royal Berkshire Hospital

Steve Stein
Senior Program Manager
Pacific Northwest National Laboratory

James Sterbenz
Professor, Resilience Against Attacks and Large-scale Disasters
University of Kansas/University of Lancaster

William Streilein
Associate Group Leader, Cyber Decision Support
via Modeling, Metrics, and Analytics
MIT Lincoln Laboratory

Iain Williams
Counselor, Security and Counter Terrorism
Science and Technology
UK Home Office

Erica Yang
Senior Computer Scientist
UK Science and Technology Facilities Council

This page left intentionally blank.

APPENDIX C: COLORS FACT SHEET

DHS Science and Technology Directorate

Collaboration on Resilience and Security

United States and the United Kingdom strategic collaboration

Important economic and defense cyber infrastructure is attacked daily around the globe. To counter this, many nations are working on approaches and technologies that could prevent or stop such attacks. The Department of Homeland Security Science and Technology Directorate and the United Kingdom (UK) Science and Technology Facilities Council are partnering under the Collaboration on Resiliency and Security (ColoRS) to pursue areas of mutual interest around core concerns, including cybersecurity of critical infrastructure, community resilience and cyber analytics. The overall intent of ColoRS is to develop and support longer term strategic collaborations, including joint projects with partners that have complementary interests and values to maximize impact and benefit. Initially, ColoRS will focus on three themes:

- **Theme 1:** Securing Infrastructure from Cyber Disruptions
- **Theme 2:** Modeling and Measuring Societal Resilience During a Cyber-Related Event
- **Theme 3:** Streaming Analytics for Effective Data Exploitation

Exploring a cyber-event from a societal resilience perspective

ColoRS will investigate these themes by exploring a scenario where a cyber-disruption occurs, heavily impacting key critical infrastructure, like power and finance and the populace of the United States (U.S.) and the UK. The collaboration will ultimately examine how resilient society would be during such a crisis and at what point would it start to break down if critical infrastructures were no longer operational? ColoRS would then determine what data exists within the infrastructures' systems and within society that may contribute to our understanding of vulnerabilities, detecting early warnings and responding to and recovering from this kind of cyber event.

Theme 1: Securing Infrastructure from Cyber Disruptions

This theme will consider—primarily be from a computer sciences perspective—the nature of the risks posed by society's dependence on cyber technology and specifically, the underlying critical infrastructures upon which services depend. It will consider both tangible (e.g., hardware) and intangible (e.g., data) elements and seek to identify previously unidentified vulnerabilities and how they could be addressed.

Theme 2: Modeling and Measuring Societal Resilience

This theme will seek to better understand the possible short and longer term effects of a cyber-related event on social structures. It will also try to clarify what we mean by resilience and identify analytical methods, approaches and metrics that could be used to measure it. The discussion will be from a computational social sciences perspective.

Theme 3: Streaming Analytics for Effective Data Exploitation

This theme will consider where applications of streaming analytics could be used to improve homeland security. For these applications, current shortfalls such as issues with privacy and information sharing will also be investigated.

Benefit to U.S. and UK research

ColoRS will provide insights into complementary research being conducted by scientists in the U.S. and UK, which will offer a broader base for publishing the results of this research. Additionally, ColoRS will leverag funding from both countries to accomplish more, faster and supplies additional sources for solutions to critical cybersecurity problems.

Homeland Security
Science and Technology

To learn more about ColoRS, please contact SandT-cyber-liaison@dhs.gov

20141105

This page left intentionally blank.

APPENDIX D: WELCOME LETTER

Homeland Security
Science and Technology

November 17, 2014

Dear Partners and Colleagues:

On behalf of myself and the U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T) I would like to welcome you to the 2014 Collaboration on Resilience and Security (ColoRS) meeting. It's an exciting time for DHS S&T, especially in the Cyber Security Division (CSD), as we continue to grow and adapt to evolving cybersecurity threats and technical needs to keep our nation secure.

For ten years, DHS and United Kingdom (UK) Home Office have worked together to identify and investigate cybersecurity threats to our communities through advancements in science and technology. The ColoRS project – co-led by DHS S&T CSD and the UK Science and Technology Facilities Council (STFC) – represents the most recent international collaboration. Under this project, CSD and STFC are working together to develop innovative ways to collaborate on research activities and to develop technologies and techniques to protect our nations' infrastructure and citizens from those who would do us harm and those disasters that would reduce our ability to protect our populace.

From a cybersecurity perspective, we need to identify research needs and encourage multi-domain and multidisciplinary teams to better anticipate threats to cyber infrastructure and mitigate the impact infrastructure failures would have on our societies. It is through collaborations like ColoRS that we are able to amplify our individual efforts and find shared solutions to combat these challenges. For these two days, we will focus on three specific themes that will benefit from the talent and dedication assembled at this meeting: *Securing Infrastructure from Cyber Disruptions, Modeling and Measuring Societal Resilience, and Streaming Analytics for Effective Data Exploitation*.

Over the course of the meeting, I ask you and the other participants to develop concepts for targeted future U.S.-UK research activities. Additionally, CSD and STFC seek to publish a special issue of a scientific journal as another output of this meeting. We will look to you to help develop the chapters for this special publication.

In closing, I am excited to work with STFC in bringing all of you together. I thank each of you for committing your time and bringing your individual expertise to these challenges, and I hope you will stay engaged with CSD and STFC as we continue this collaboration.

Best Regards,

Douglas Maughan, PhD
Director
Cyber Security Division
Science and Technology Directorate
U.S. Department of Homeland Security

APPENDIX E: MEETING AGENDA

Agenda

US-UK Program on Collaboration on Resiliency and Security (ColoRS) Working Meeting

November 17th and 18th, 2014 | Washington, DC

Sponsored by:
U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T)
and
U.K. Science and Technology Facilities Council (STFC)

PRE-EVENT (NOVEMBER 16):

6-8pm **No-Host Welcome Happy Hour**
Gordon Biersch
900 F Street NW, Washington, DC 20004

DAY 1 (NOVEMBER 17)

8:00 am **Registration and networking**

8:30 am **Welcome**
Dr. Douglas Maughan
Director, Cyber Security Division, DHS S&T

8:35 am **Opening Remarks from the US**
Dr. Robert Griffin
Deputy Under Secretary, DHS S&T

8:45 am **Welcome and Opening Remarks from the UK**
Dr. Bernard Silverman
Chief Scientific Adviser, UK Home Office

9:00 am **Event Overview and Introduction**
- Dr. Bryan Edwards
  Programme Leader, STFC
- Dr. Joseph Kielman
  Program Manager, DHS S&T
- Ms. Emily Saulsgiver
  Program Support, DHS S&T

9:30 am **MORNING COFFEE AND NETWORKING BREAK**

10:00 am **Breakout Sessions on Research Needs**
- Breakout Theme 1 – Securing Infrastructure from Cyber Distributions
- Breakout Theme 2 – Modeling and Measuring Societal Resilience
- Breakout Theme 3 – Streaming Analytics for Effective Data Exploitation

12:00 pm **BREAK FOR LUNCH AND GALLERY WALK**
At the end of each breakout session, each group will be required to post concepts and ideas into their section of the Gallery Walk. All participants will be encouraged to review the other sessions' progress and leave comments for their consideration during the next breakout session.

6

1:00 pm	**Breakout Sessions Continued** (project designs to address research needs and policy issues) • Breakout Theme 1 – Securing Infrastructure from Cyber Distributions • Breakout Theme 2 – Modeling and Measuring Societal Resilience • Breakout Theme 3 – Streaming Analytics for Effective Data Exploitation
2:30 pm	**AFTERNOON COFFEE AND GALLERY WALK**
3:00 pm	**Breakout Sessions Continued** (project designs to address research needs and policy issues)
4:30 pm	**Wrap-Up** • Summary of the highpoints from Day 1 (each group gets 8 minutes) • Review agenda and actions for Day 2
7:30 pm	**STFC-hosted Conference Dinner** HAMILTON CROWNE PLAZA 1001 14th Street NW Washington, DC 20005

DAY 2 (NOVEMBER 18)

8:00 am	**Sign-In**
8:30 am	**Welcome Back, Recap of Day 1, and Expectations for the Day** • Dr. Bryan Edwards Programme Leader, STFC • Dr. Joseph Kielman Program Manager, DHS S&T • Ms. Emily Saulsgiver Program Support, DHS S&T
8:45 am	**Breakout Groups Reconvene and Prepare for Report Out**
9:45 am	**COFFEE AND GALLERY WALK**
10:00 am	**Breakout Session 1 Summary** • Research Topic • Objective and key questions • Policy issues • Project design • Project team • Group discussion
10:45 am	**Breakout Session 2 Summary** • Research Topic • Objective and key questions • Policy issues • Project design • Project team • Group discussion
11:30 am	**Breakout Session 3 Summary** • Research Topic

- Objective and key questions
- Policy issues
- Project design
- Project team
- Group discussion

12:15 pm **BREAK FOR LUNCH**

1:15 pm **Break Out Sessions Continued**

- Breakout Theme 1 – Securing Infrastructure from Cyber Distributions
- Breakout Theme 2 – Modeling and Measuring Societal Resilience
- Breakout Theme 3 – Streaming Analytics for Effective Data Exploitation

2:30pm **COFFEE AND GALLERY WALK**

3 pm **Break Out Sessions Continued**

- Breakout Theme 1 – Securing Infrastructure from Cyber Distributions
- Breakout Theme 2 – Modeling and Measuring Societal Resilience
- Breakout Theme 3 – Streaming Analytics for Effective Data Exploitation

3:30 pm **Final Concept Presentation:** Securing Infrastructure from Cyber Distributions

4pm **Final Concept Presentation:** Modeling and Measuring Societal Resilience

4:30pm **Final Concept Presentation:** Streaming Analytics for Effective Data Exploitation

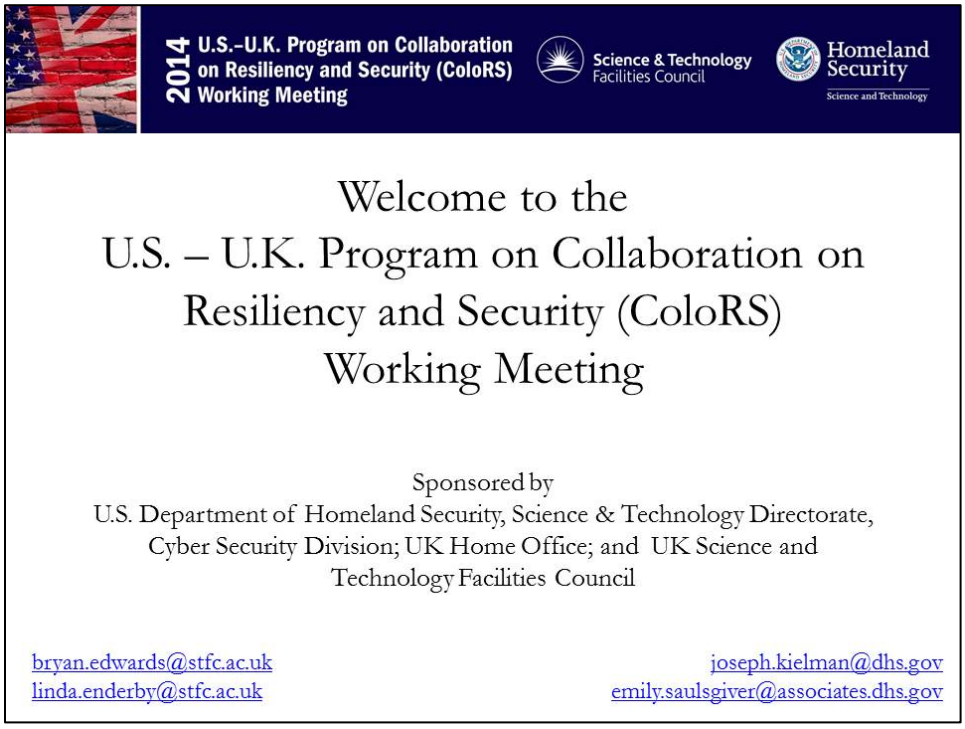
5pm **Path Forward and Final Remarks**

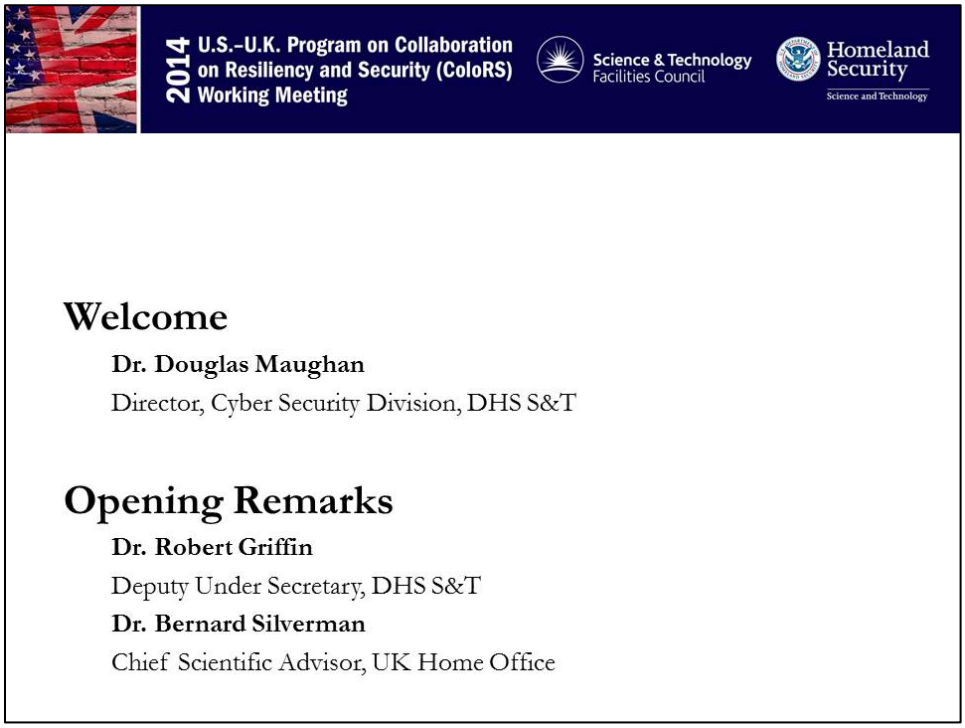
- Dr. Bryan Edwards
  Programme Leader, STFC
- Dr. Joseph Kielman
  Program Manager, DHS S&T

5:30 pm **Adjourn**

This page left intentionally blank

APPENDIX F: PRESENTATIONS FROM MEETING



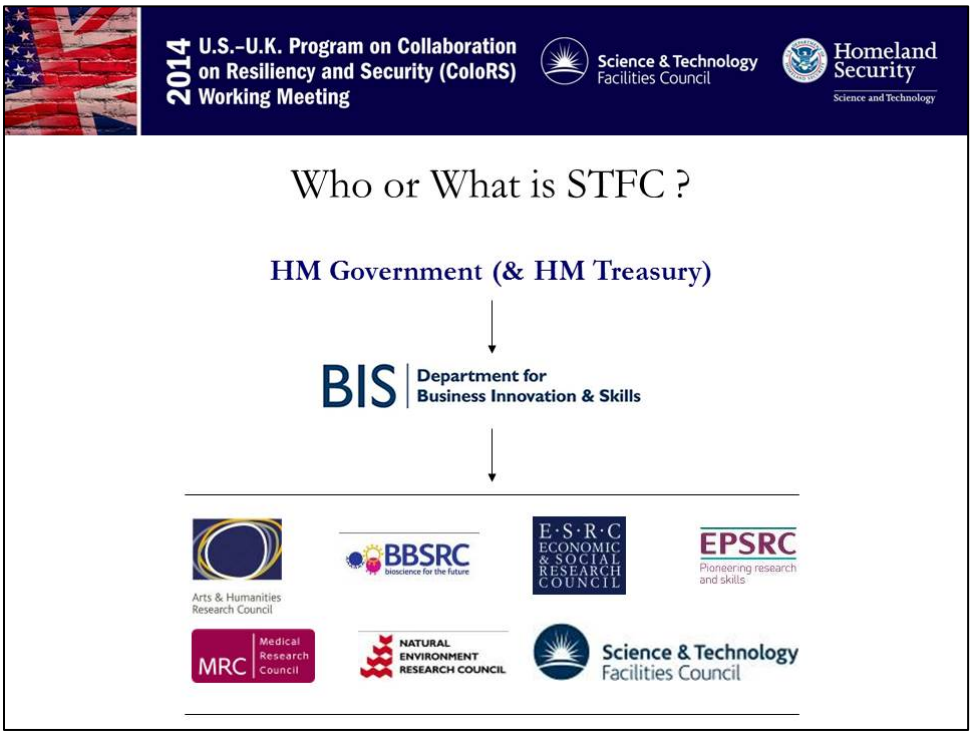


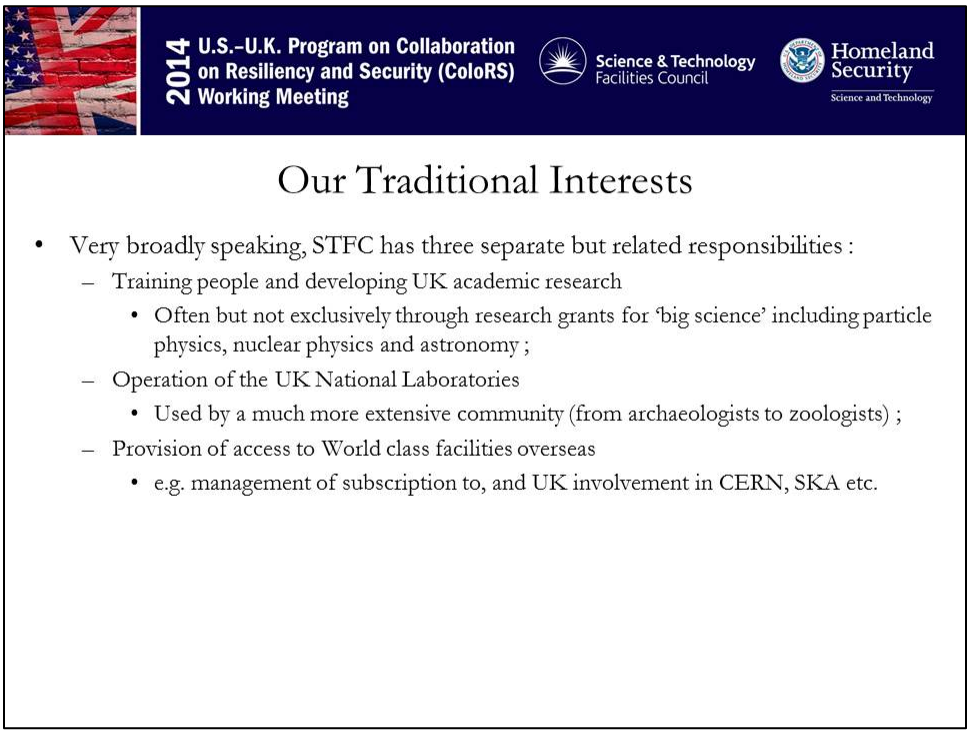
2014 U.S.–U.K. Program on Collaboration on Resiliency and Security (ColoRS) Working Meeting
Science & Technology Facilities Council
Homeland Security Science and Technology

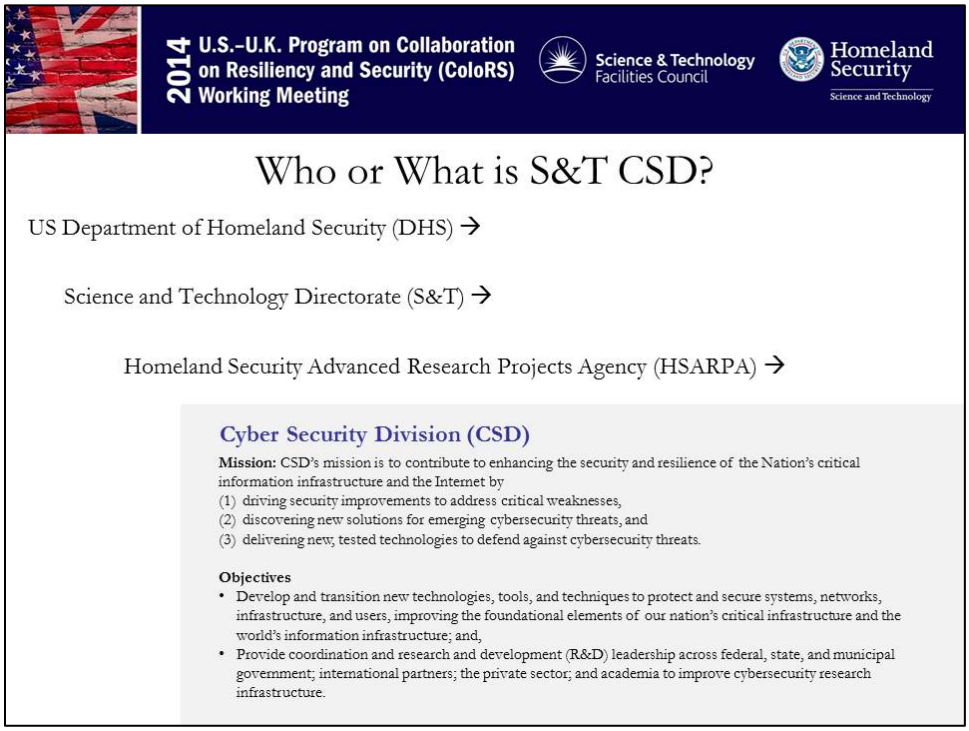
- Bathroom is on the…
- Coffee may be found…
- Please turn your cellphone to silent.
- Lunch is on your own. See registration table for a list of nearby eateries.
- A final meeting report will be issued and shared with the participants.

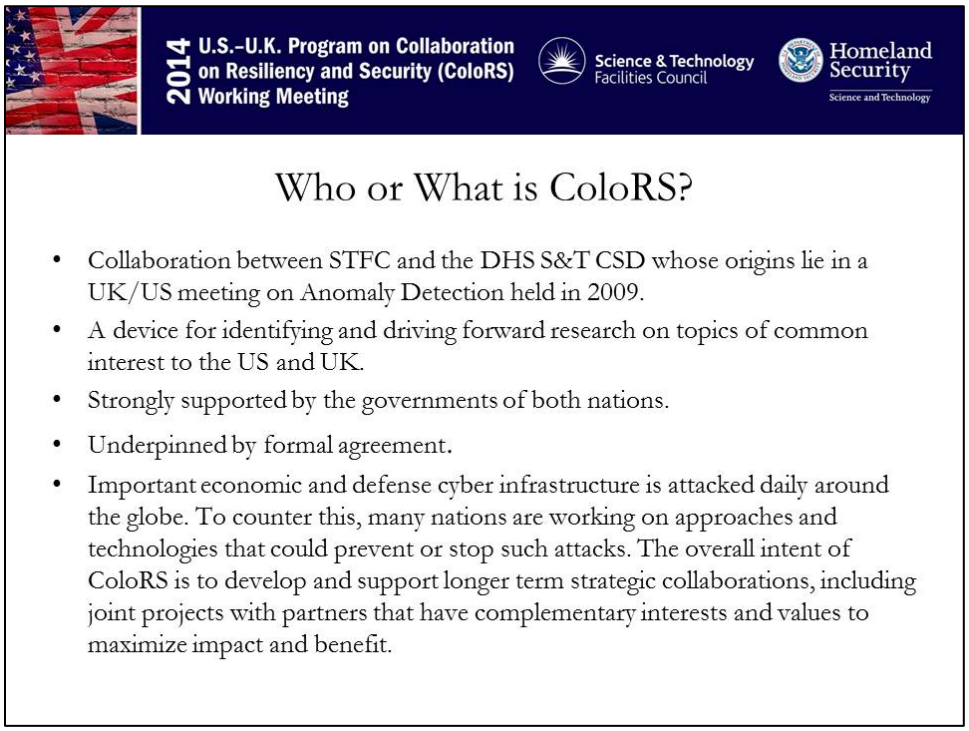
2014 U.S.–U.K. Program on Collaboration on Resiliency and Security (ColoRS) Working Meeting
Science & Technology Facilities Council
Homeland Security Science and Technology

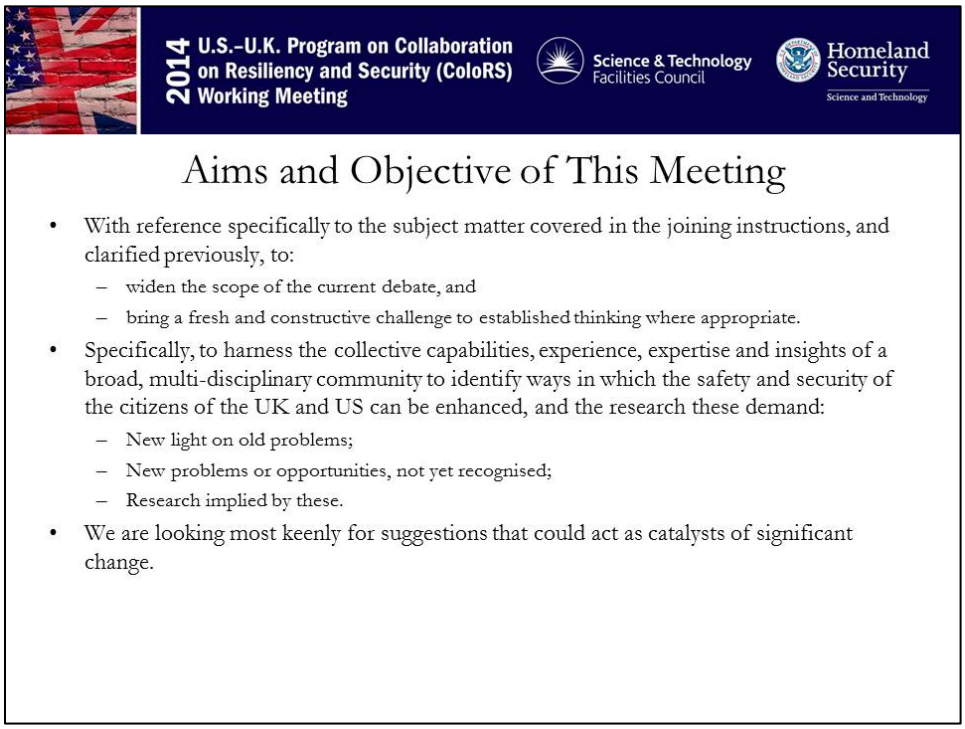
Introductions and Welcome


2014 U.S.–U.K. Program on Collaboration on Resiliency and Security (ColoRS) Working Meeting
Science & Technology Facilities Council
Homeland Security Science and Technology
Who or What is STFC ?
HM Government (& HM Treasury)
BIS Department for Business Innovation & Skills
Arts & Humanities Research Council
BBSRC bioscience for the future
E·S·R·C ECONOMIC & SOCIAL RESEARCH COUNCIL
EPSRC Pioneering research and skills
MRC Medical Research Council
NATURAL ENVIRONMENT RESEARCH COUNCIL
Science & Technology Facilities Council


2014 U.S.–U.K. Program on Collaboration on Resiliency and Security (ColoRS) Working Meeting
Science & Technology Facilities Council
Homeland Security Science and Technology
Our Traditional Interests
• Very broadly speaking, STFC has three separate but related responsibilities :
– Training people and developing UK academic research
• Often but not exclusively through research grants for 'big science' including particle physics, nuclear physics and astronomy ;
– Operation of the UK National Laboratories
• Used by a much more extensive community (from archaeologists to zoologists) ;
– Provision of access to World class facilities overseas
• e.g. management of subscription to, and UK involvement in CERN, SKA etc.

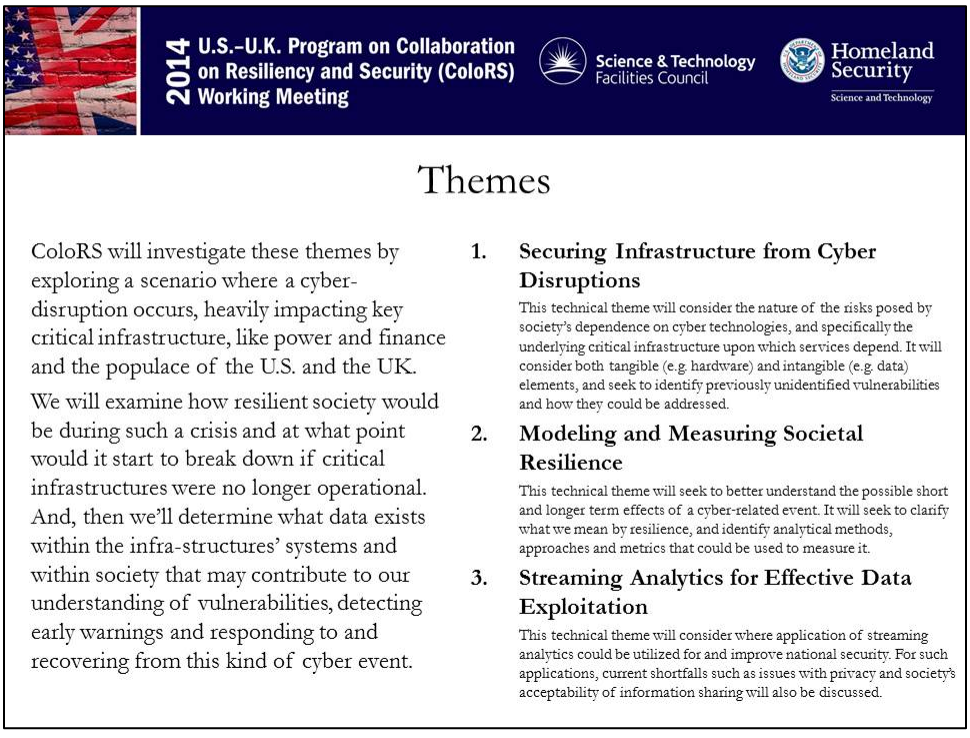

2014 U.S.–U.K. Program on Collaboration on Resiliency and Security (ColoRS) Working Meeting
Science & Technology Facilities Council
Homeland Security Science and Technology
Who or What is S&T CSD?
US Department of Homeland Security (DHS) →
Science and Technology Directorate (S&T) →
Homeland Security Advanced Research Projects Agency (HSARPA) →
Cyber Security Division (CSD)
Mission: CSD's mission is to contribute to enhancing the security and resilience of the Nation's critical information infrastructure and the Internet by
(1) driving security improvements to address critical weaknesses,
(2) discovering new solutions for emerging cybersecurity threats, and
(3) delivering new, tested technologies to defend against cybersecurity threats.
Objectives
• Develop and transition new technologies, tools, and techniques to protect and secure systems, networks, infrastructure, and users, improving the foundational elements of our nation's critical infrastructure and the world's information infrastructure; and,
• Provide coordination and research and development (R&D) leadership across federal, state, and municipal government; international partners; the private sector; and academia to improve cybersecurity research infrastructure.

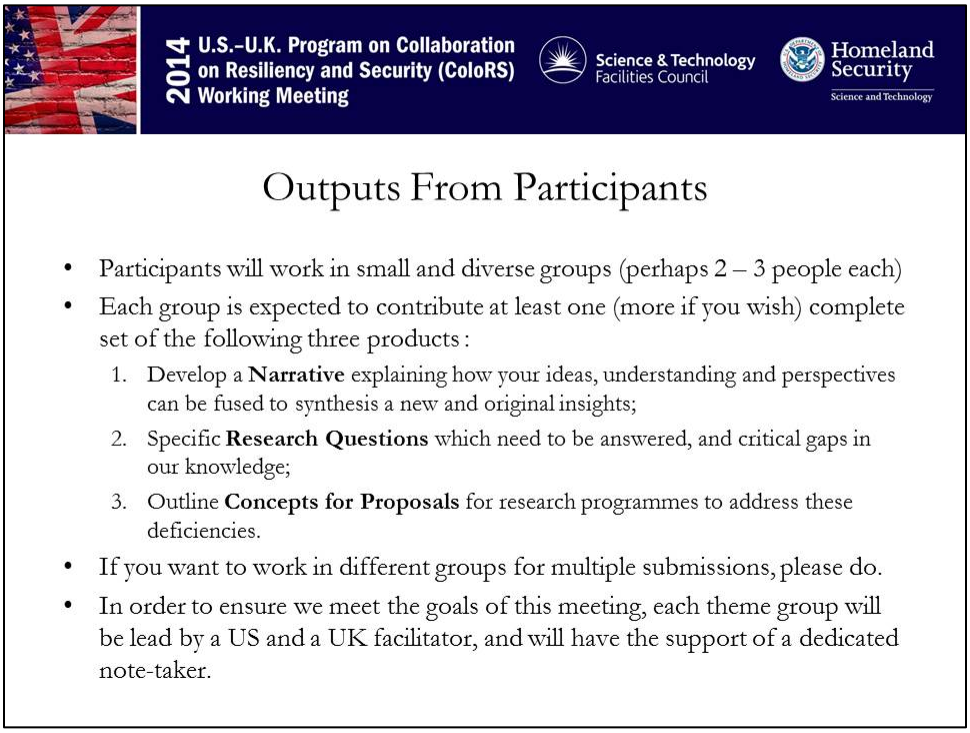

2014 U.S.–U.K. Program on Collaboration on Resiliency and Security (ColoRS) Working Meeting
Science & Technology Facilities Council
Homeland Security Science and Technology
Who or What is ColoRS?
• Collaboration between STFC and the DHS S&T CSD whose origins lie in a UK/US meeting on Anomaly Detection held in 2009.
• A device for identifying and driving forward research on topics of common interest to the US and UK.
• Strongly supported by the governments of both nations.
• Underpinned by formal agreement.
• Important economic and defense cyber infrastructure is attacked daily around the globe. To counter this, many nations are working on approaches and technologies that could prevent or stop such attacks. The overall intent of ColoRS is to develop and support longer term strategic collaborations, including joint projects with partners that have complementary interests and values to maximize impact and benefit.

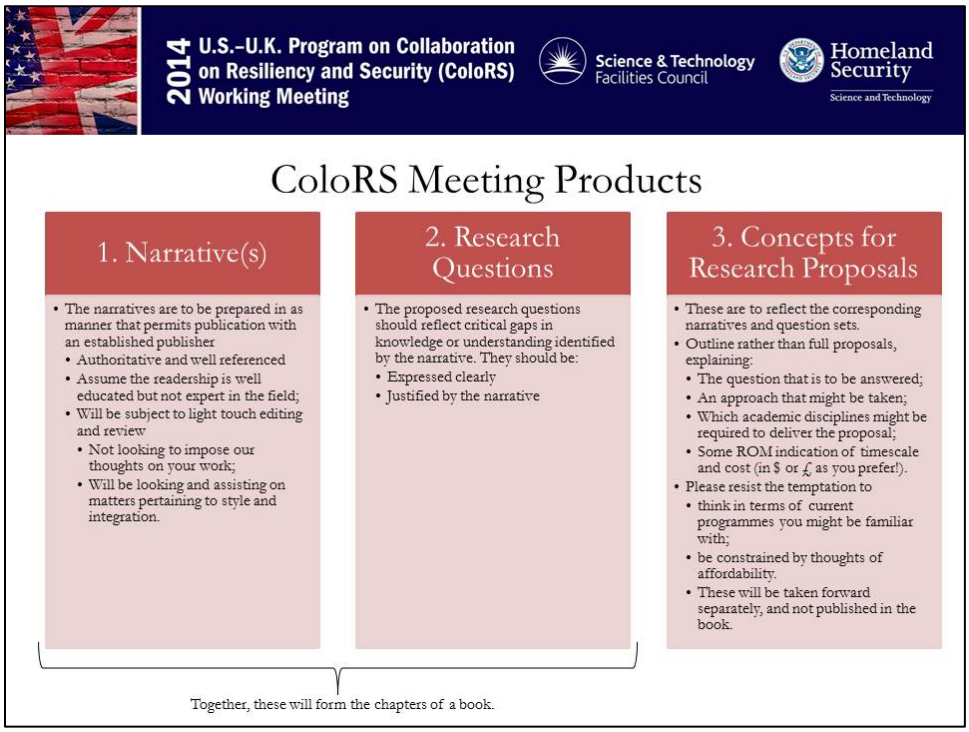

2014 U.S.–U.K. Program on Collaboration on Resiliency and Security (ColoRS) Working Meeting
Science & Technology Facilities Council
Homeland Security Science and Technology
Aims and Objective of This Meeting
• With reference specifically to the subject matter covered in the joining instructions, and clarified previously, to:
– widen the scope of the current debate, and
– bring a fresh and constructive challenge to established thinking where appropriate.
• Specifically, to harness the collective capabilities, experience, expertise and insights of a broad, multi-disciplinary community to identify ways in which the safety and security of the citizens of the UK and US can be enhanced, and the research these demand:
– New light on old problems;
– New problems or opportunities, not yet recognised;
– Research implied by these.
• We are looking most keenly for suggestions that could act as catalysts of significant change.

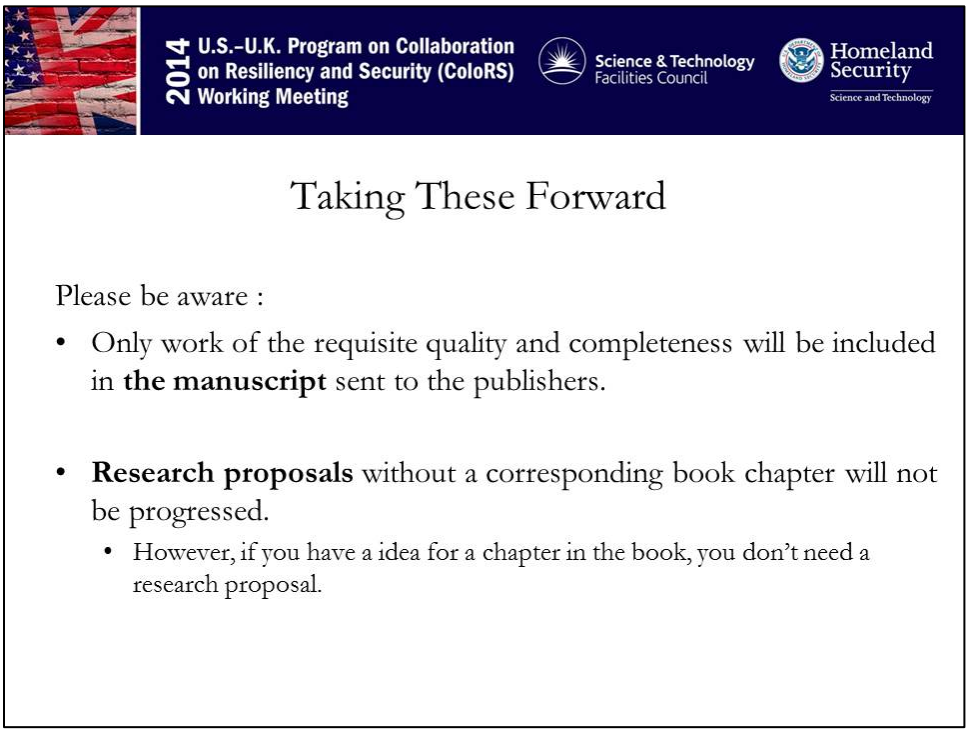

2014 U.S.–U.K. Program on Collaboration on Resiliency and Security (ColoRS) Working Meeting
Science & Technology Facilities Council
Homeland Security Science and Technology
Agenda
Day 01 (November 17th)
8:00 am Registration and networking
8:30 am Welcome
8:35 am Opening Remarks from the US
8:45 am Welcome and Opening Remarks from the UK
9:00 am Event Overview and Introduction
9:30 am MORNING COFFEE AND NETWORKING BREAK
10:00 am Breakout Sessions on Research Needs
12:00 pm BREAK FOR LUNCH AND GALLERY WALK
1:00 pm Breakout Sessions Continued
2:30 pm AFTERNOON COFFEE AND GALLERY WALK
3:00 pm Breakout Sessions Continued
4:30 pm Wrap-Up
5:00 pm Adjourn
7:30 pm STFC-hosted Conference Dinner (Hamilton Crowne Plaza – Franklin Park Room)

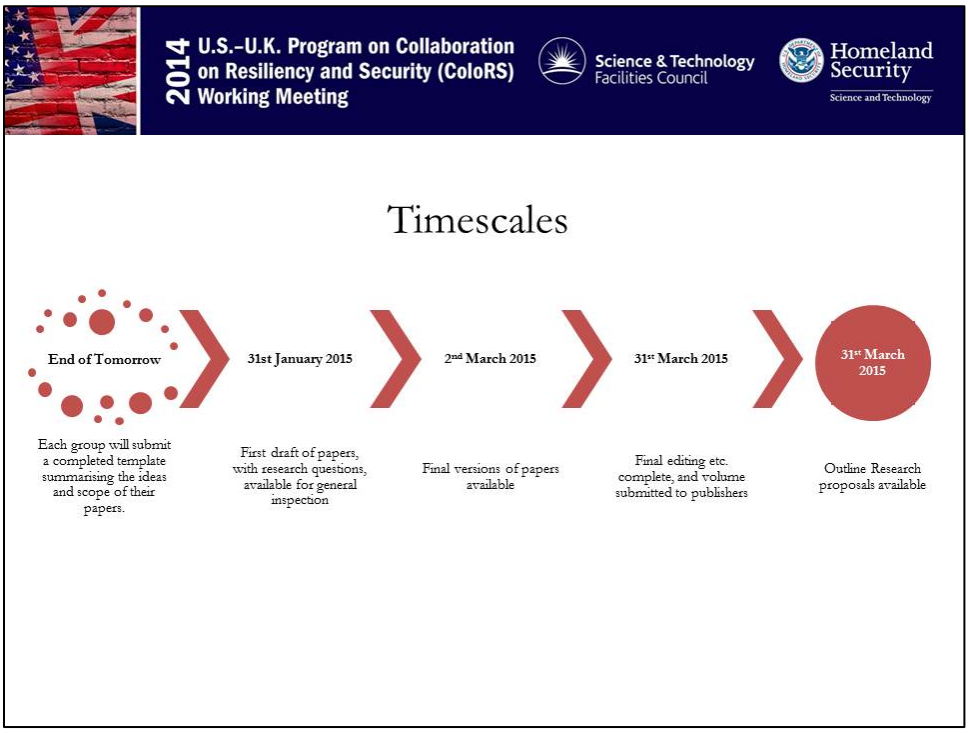

2014 U.S.–U.K. Program on Collaboration on Resiliency and Security (ColoRS) Working Meeting
Science & Technology Facilities Council
Homeland Security Science and Technology
Agenda
Day 02 (November 18th)
8:00 am Sign-In
8:30 am Welcome Back, Recap of Day 1, and Expectations for the Day
8:45 am Breakout Groups Reconvene and Prepare for Report Out
9:45 am COFFEE AND GALLERY WALK
10:00 am Breakout Theme 1 Summary
10:45 am Breakout Theme 2 Summary
11:30 am Breakout Theme 3 Summary
12:15 pm BREAK FOR LUNCH AND GALLERY WALK
1:15 pm Break Out Sessions Continued
2:30pm COFFEE AND GALLERY WALK
3:00 pm Break Out Sessions Continued
3:30 pm Final Concept Presentation: Securing Infrastructure from Cyber Distributions
4:00 pm Final Concept Presentation: Modeling and Measuring Societal Resilience
4:30pm Final Concept Presentation: Streaming Analytics for Effective Data Exploitation
5:00 pm Path Forward and Final Remarks
5:30 pm Adjourn


2014 U.S.–U.K. Program on Collaboration on Resiliency and Security (ColoRS) Working Meeting
Science & Technology Facilities Council
Homeland Security Science and Technology
Themes
ColoRS will investigate these themes by exploring a scenario where a cyber-disruption occurs, heavily impacting key critical infrastructure, like power and finance and the populace of the U.S. and the UK.
We will examine how resilient society would be during such a crisis and at what point would it start to break down if critical infrastructures were no longer operational. And, then we'll determine what data exists within the infra-structures' systems and within society that may contribute to our understanding of vulnerabilities, detecting early warnings and responding to and recovering from this kind of cyber event.
1. Securing Infrastructure from Cyber Disruptions
This technical theme will consider the nature of the risks posed by society's dependence on cyber technologies, and specifically the underlying critical infrastructure upon which services depend. It will consider both tangible (e.g. hardware) and intangible (e.g. data) elements, and seek to identify previously unidentified vulnerabilities and how they could be addressed.
2. Modeling and Measuring Societal Resilience
This technical theme will seek to better understand the possible short and longer term effects of a cyber-related event. It will seek to clarify what we mean by resilience, and identify analytical methods, approaches and metrics that could be used to measure it.
3. Streaming Analytics for Effective Data Exploitation
This technical theme will consider where application of streaming analytics could be utilized for and improve national security. For such applications, current shortfalls such as issues with privacy and society's acceptability of information sharing will also be discussed.


2014 U.S.–U.K. Program on Collaboration on Resiliency and Security (ColoRS) Working Meeting
Science & Technology Facilities Council
Homeland Security Science and Technology
Outputs From Participants
• Participants will work in small and diverse groups (perhaps 2 – 3 people each)
• Each group is expected to contribute at least one (more if you wish) complete set of the following three products :
1. Develop a Narrative explaining how your ideas, understanding and perspectives can be fused to synthesis a new and original insights;
2. Specific Research Questions which need to be answered, and critical gaps in our knowledge;
3. Outline Concepts for Proposals for research programmes to address these deficiencies.
• If you want to work in different groups for multiple submissions, please do.
• In order to ensure we meet the goals of this meeting, each theme group will be lead by a US and a UK facilitator, and will have the support of a dedicated note-taker.


2014 U.S.–U.K. Program on Collaboration on Resiliency and Security (ColoRS) Working Meeting
Science & Technology Facilities Council
Homeland Security Science and Technology
ColoRS Meeting Products
1. Narrative(s)
• The narratives are to be prepared in as manner that permits publication with an established publisher
• Authoritative and well referenced
• Assume the readership is well educated but not expert in the field;
• Will be subject to light touch editing and review
• Not looking to impose our thoughts on your work;
• Will be looking and assisting on matters pertaining to style and integration.
2. Research Questions
• The proposed research questions should reflect critical gaps in knowledge or understanding identified by the narrative. They should be:
• Expressed clearly
• Justified by the narrative
3. Concepts for Research Proposals
• These are to reflect the corresponding narratives and question sets.
• Outline rather than full proposals, explaining:
• The question that is to be answered;
• An approach that might be taken;
• Which academic disciplines might be required to deliver the proposal;
• Some ROM indication of timescale and cost (in $ or £ as you prefer!).
• Please resist the temptation to
• think in terms of current programmes you might be familiar with;
• be constrained by thoughts of affordability.
• These will be taken forward separately, and not published in the book.
Together, these will form the chapters of a book.


2014 U.S.–U.K. Program on Collaboration on Resiliency and Security (ColoRS) Working Meeting
Science & Technology Facilities Council
Homeland Security Science and Technology
Taking These Forward
Please be aware :
• Only work of the requisite quality and completeness will be included in the manuscript sent to the publishers.
• Research proposals without a corresponding book chapter will not be progressed.
• However, if you have a idea for a chapter in the book, you don't need a research proposal.


2014 U.S.–U.K. Program on Collaboration on Resiliency and Security (ColoRS) Working Meeting
Science & Technology Facilities Council
Homeland Security Science and Technology
Timescales
End of Tomorrow
Each group will submit a completed template summarising the ideas and scope of their papers.
31st January 2015
First draft of papers, with research questions, available for general inspection
2nd March 2015
Final versions of papers available
31st March 2015
Final editing etc. complete, and volume submitted to publishers
31st March 2015
Outline Research proposals available

APPENDIX G: THEME DISCUSSION DETAILS

THEME 1: SECURING INFRASTRUCTURE FROM CYBER DISRUPTIONS

Acceptance of risk is different at different levels. Would defensive measures differ accordingly? People have to be enabled to make decisions; this has dramatic implications. What are the time requirements and limitations? Costs must be incorporated over a life cycle.

The complex interdependencies of various components form an important part of the architecture and design for resilient cyber systems. What happens if we cannot get parts? What are the external dependencies? Do we even have the ability to analyze this?

How do we create resiliency? It involves monitoring and metrics, technology and people. It is affected by the time or phase of response. The infrastructure is currently evolving. Is it possible to start from a clean slate and integrate over time, with security built in from day one?

Equally important are the roles, responsibilities, and behavior of individuals in organizations in relationship to technology systems. Accountability must lead to action. Case studies could help us understand this component.

Security is an enabler for resilience. A DHS initiative is looking at it from the perspective of all-hazards risk modeling. How do we share information with those who are going to do something with it?

Both the UK and the US have lists of key infrastructure binned by critical infrastructure sector. One of the challenges is not having a good understanding of the legacy systems and consequences of impacts on critical infrastructure. We lack a comprehensive model and framework to predict ripple/cascading effects. Can we address scale and pace, perhaps through automation? Bottlenecks must be identified.

We need to consider societal response to support decision-making. Who is warned and how? Social media represents both an opportunity and a challenge. Uncertainty abounds in how to use it and what outcomes it supports. What must be shared for societies to be more resilient?

Another challenge is ownership: who owns the critical infrastructure? It may even be owned by foreign entities. The private sector is more concerned about protecting customers and the bottom line. Normally a company wants to fix its own issues as opposed to going to the government for help. Unfortunately, companies may not have the internal capabilities to address issues of security. While many sectors are becoming familiar such issues, and larger companies are well along, smaller companies may struggle. Most insurance companies do not address or understand cybersecurity. Maybe cybersecurity should be its own critical infrastructure.

There are two main threads to securing infrastructure from cyber disruptions: insight/situational awareness and operation. In the area of insight and situational awareness, where is the interconnectivity and the sources of vulnerability now? How might the infrastructure evolve? At what scale must we understand risk exposure: individually, nationally, globally? What about the supply chains? What comprises the system, its assets, and its brand? How will its failure affect markets? There may be opportunities for analytics and models in this area.

In the area of operations, how can we design a system to be more resilient? How can we detect threats right away, the earlier the better? Do we need to know that we have a problem or the actual nature of the problem? Do we want to know who else may be seeing the same problem?

When it comes to response and recovery, part of the definition of resilience is to be able to recover better. For example, the future Internet could have resilient mechanisms built in. The Securities Industry and Financial Markets Association held two Quantum Dawn Exercises to enable both individual firms and the financial sector as a whole to test their response plans to maintain effective and orderly markets and protect clients in the event of a systematic cyber-attack.

Timeliness is another issue. Things must be done quickly, automatically. The NASDAQ was hacked but the system could not be taken offline to determine the problem. Instead, it had to operate through the attack while it was being fixed. In other cases, companies may have the software to detect an attack but have disabled parts of it because the software slows down other processes. Cost is another deterrent to effectively running detection software.

Any modeling must include the ability to learn. We should be able to model the nature of attacks, identify patterns, and make decisions on what to do. Being able to respond, recover, and adapt will lead to improved infrastructure.

How can we encourage companies and governments to invest in cybersecurity? Insurance is one thing but incentives also form a possibility. Is public pressure enough of an incentive to do something? Or, will companies only respond once they have been attacked? Even if the government provided detection information, some companies would rather not know they have code vulnerability because then they would be obligated to do something. Can we offer incentives to the suppliers to deliver more resilient products?

A lot of older infrastructure has more of an assemblage of code–part of the code was developed over time in response to disasters. Building systems of dependent components includes both software and hardware (any logic-bearing components). The integrity of the building blocks matters.

When it comes to cloud computing, most decisions being made about public and private infrastructure is entrusted to an external party. Critical infrastructure providers are creating their own internal cloud. The challenge is buying security as a service. The companies think they have transferred the risk to the

external party. There is a divorce between those who understand the risk and those making decisions. We need to connect the infrastructure and the mission. This is where the risk is found. We have look at resilience and quality control at the lower level.

Thinking could be organized according to the US National Institute for Standards and Testing's framework of information sharing: identify, protect, detect, respond (remediate), recover, and adapt. We can start by being proactive. We must gain an institutional understanding of what needs to be protected (risk assessment, both threat and impact). This understanding includes the infrastructure (hardware, software) and assets (cooperative versus non-cooperative), as well as weaknesses and vulnerabilities. Companies could map the mission down to the infrastructure and determine how to monitor performance to protect and defend.

Safety and security are separated. It's not until safety is impacted that security is an issue. Perhaps a system should not be considered "safe" unless it is secure. The safety community has a very clear assessment process. The security community needs convincing science and data to show the connection. We lack decent and insightful models, as well as the standards, to show the level of "security" of something. What could we do better if we knew all this? We should be able to achieve aspirational resilience, evolving the system into a better position.

Prediction is based on a reactive solution. Therefore, we must also be ready to react. Once we detect undesirable activities, we must be able to determine the consequences. What is the threat? What's the interface between policy and action? Can we cause a problem and go through the process of sorting things out? Do we know how to re-establish the infrastructure? Can we share what we did to ensure the system is in better shape for the future?

The challenge for communication is the speed at which the event will happen. What information does the infrastructure owner have? What do the operators need or have? What does the responder have or need? What does the community have and need? What about other businesses? The three most important factors are the time, the quality of the information, and the destination of the information. A problem is the authority over the data being using–data is only as good as the people who use and implement it. We need to determine a scalable way of sharing information so people who receive it know what to do with it–the data is a prop for actions. Data must drive the response.

Particularly difficult problems include the following:

- Risk indicators and probability
- Ways of being and what drives them, which varies greatly across society
- The ownership and maintenance of data sets for resiliency
- Incorporating adaptation
- The notion of continuous exercises–red-teaming non-stop

- Societal change, critical sector failure, and transparency
- Control of the organization and its goals post-recovery
- The level of dynamic movement and ability of organizations to work strategically

THEME 2: MODELING AND MEASURING SOCIETAL RESILIENCE

One area to consider is the interplay between societal and network systems. Differential impacts are likely on different types of societies. Different players will have different responses and feel different effects. For example, the Amish are likely to feel minimal effects from a cyber-disruption. How will people respond—get food, get money for food? How can we achieve a new normal without cyber attached to it? How does the impact and the societal reaction change as the event continues—one day, one week, one month, six months, and longer?

Another area of consideration will be leadership and governance. Whoever governs must have credibility and legitimacy, and different social groups have different leaders with those traits. Are these leaders predictable? Who will emerge to lead adaptation to the new situation following a cyber-event? The scales will differ, and temporal dimensions should be considered. How does leadership evolve without information systems attached? Whose responsibility is all this?

A cyber-attack requires an interdisciplinary approach. We might use established models and insights from other disciplines to understand cyber-events as similar or analogous to phenomena we already understand. Do we need a top-down or bottom-up approach, and where will they meet?

Defining failure will be key. How will we discern what has happened? What are the measures and indicators of failure? How are they monitored, given the dynamic nature of the "normal state"? It has been said that the "normal" condition of a network is to be under constant attack, but "normal" is not universal and might be defined differently by smaller groups. How does a large entity restore one "normal" to all?

Are there realistic partial loss scenarios as opposed to just interesting ideas? We may have to stay within larger categories instead of being too specific. We cannot lay out every possible event, so the study of the categories of events could provide scenario planning with broader applications. Too often scenarios are imagined that have little or no grounding in the actual behavior of people in similar events. For example, perhaps communication is not down, but it is unreliable and unofficial, which could undermine trust. People might look for information from Twitter rather than official channels. In this case Twitter would have the credibility and timeliness, but it may not be accurate.

How do the law-abiding and non-law-abiding players respond differentially to events? The actual and perceived cause of the event shapes the response. For example, a terrorist attack will be seen as a shared communal threat. An attack by an anonymous entity may have many who are sympathetic to the

attackers and are therefore less likely to cooperate in the recovery. One approach might be to start with capacities and capabilities, as opposed to starting with scenarios and working with vulnerabilities.

Another issue will be the ability to communicate in common terms. Do multiple stakeholders discussing these issues have common ground and definition to facilitate their discussion? We must define the aspects of resilience to know where we can agree and disagree and facilitate coming together in overlapping areas of interest and concern.

It may be that we need categories of function rather than categories of failure. For instance, losing the ability to go to work if the Internet is down cuts across multiple types of workplaces. Would it be wise to force the Internet to cache and operate locally, reducing reliance on overall, widespread connectivity? We would be reducing the reliance on global connectivity to maintain local function.

Do we really understand how dependent we are on cyber systems? Could we revert to doing complex situations without a cyber system, or has society fundamentally changed? What is the tipping point/breaking point of society? How quickly could people be reconnected? How would local governments cope failing knowledge from higher up? Could we use indicators to show which segments of society are more vulnerable?

THEME 3: ANALYTICS FOR EFFECTIVE DATA EXPLOITATION

While the goal may be streaming data—as real-time as possible—the reality is that data are generated in an unorganized manner and only occasionally in tabular form and time stamped. Analytical models applied to such raw data can only generate warnings or prioritized information. These models must include both the incoming data and the methods of processing them. Given enough power, we could construct a model that would identify holes or vulnerabilities. Visualizations and database structures could be factored into security and vice versa.

But there are characteristics beyond data and processing. Consider scale. How do we secure a large enterprise? Gateway routers generate streams of data in enormous volume, yet every industry's inputs and outputs can be different. In addition, enterprises evolve independently. Because of this complexity, we do not look for failures in signatures. Instead, we look for patterns that are suggestive of failure, probabilistic of failure. One part of the resilience problem is monitoring for threats, abnormalities of some kind. Clever adversaries hide the abnormalities in the noise.

How can we utilize private data that is rarely if ever seen by government agencies? How can we erect barriers between organizations that enable information sharing with adequate protection? Machine-learning runs better the more data it has, but useful data may be limited, so the process is slow.

From a mathematical point of view, streaming data has many variables, even if limited to a 6-month period. Another problem in cybersecurity is the failure to take into account the emergency responder

approach. Information comes at the federal or state level. Isolated organizations respond differently. Anti-virus and anti-spam companies have been more successful in solving this problem—they may have isolated victims but one patch fits all.

Policy can solve some of these problems. It can constrain the types of questions that can be asked of the data. A database protected by cryptography can be set up with levels of authority, and some users can access deeper. Unfortunately, real-time data comes faster than one person can read it. For a system on a grand scale, aggregating this information is impossible at the size and expertise required. A distributed infrastructure might be better.

Access rights and the ability to monitor must be balanced. Who will know if the database has been compromised? When a system is compromised, policies cannot respond fast enough. Today, chaos is normal, and the normal state of a network is to be attacked. The definition of "normal" should go deeper than in a mechanical system.

Evolutionary adaptation would encompass a constant reaction to what is happening so there is no question as to what is normal or abnormal. Resilience implies we are coming back to a preferred state. Is that what we want? We need to make sure we are measuring the right things. If we see a pattern that has no precedence, that pattern could be examined and added to the database so that correlations grow with time.

If we divide the infrastructure into layers, what might be normal in one place could be abnormal elsewhere. What could be small in one layer could become larger in others. Only a human will know whether a change of any kind is important.

We care about streaming data because it helps us identify something bad. The impact on infrastructure means denial of service, theft, and disruption of critical infrastructures. How resilient is resilient enough? What are the metrics? If we are using streaming for early threat detection, what analysis is needed to determine that something is happening? If something triggers a warning, then we need to be able to go back and mine the data to determine what is happening. We can also look at the growth of abnormalities. If the rate is really fast, we must shut down everything and focus on the problem. But, what if we cannot shut everything down? Early recognition, emergency monitoring, and then appropriate response are key. Historical analysis can be undertaken when we have the luxury of time.

Black swan events are by definition not included in our models. What relevant data should we be collecting? For example, should we look at employee absences? If a cyber-expert is not around, is the company for which he works suddenly more vulnerable? Maybe we should be monitoring a broader set of things. We are looking at slow, methodical, and smart opponents. If we always monitor the same things, our success at identifying attacks will be low.

Look at the human side of the equation. We have three categories of actors:

1. Operators for monitoring, heavily assisted by automated methods. They deal with streaming data.
2. Analysts, who look into special cases and use historical data, they are more skilled and knowledgeable.
3. Modelers, who check to make sure our decision processes and models still work, create new models, and identify new data sources. They train the other two categories.

What tools and skills does each category need?

If we cannot fend off a threat, it is better to adapt to its presence. We need to differentiate between cause and effect. Because we cannot move quickly enough to isolate the cause, we take Draconian action. If we could rapidly find the cause, we could react more appropriately. Diagnostics might allow us to make decisions without knowing the causality.

The current system is not set up to take into account back channels. Adversaries can cut them off, slow down the system, and transmit information via a different route. Back channels must be designed into the system. We need to be able deny service it faster in an emergency. Health monitoring is poor stepchild of surveillance, but very critical.

This page left intentionally blank.

APPENDIX H: PARTICIPANT FEEDBACK

Participants at the ColoRS working meeting were asked for feedback. They supplied the following remarks:

- Very useful, very interesting, very grateful to have been invited to take part.
- Great international-ism – adds an excellent dimension to research
- Fantastic interaction with people from different disciplines. Opportunities to work with people I'd rarely engage. Excellent group dynamics—constructive, collegiate, and intellectually stimulating exchange. Great facilitation, more directed discussion on key themes at the outset and strict timekeeping on presentations would be very minor improvements to an excellent event.
- Great brainstorm meeting, many experts who all know what they are talking about. This is the place where big ideas come out.
- Great organizers, facilitators, and moderators—been to [other federal agency] meetings that weren't this good.
- Great opportunity for multi-disciplinary collaboration.
- Useful to bring together multiple-field experts, but especially researchers and people familiar with actual uses
- Amazing meeting! Wonderful balance of creative communication, brainstorming, and focused work on a meaningful product.
- Really fantastic for a law enforcement practitioner to have the opportunity to engage with, learn from, and develop practical relationships with excellent people from multiple disciplines.
- Really liked the structure. The moderators were excellent at facilitating discussion driving towards concrete expression of ideas. Brainstorming was intense and might have been broken up by topical presentations. Overall: great!
- Great chance to mix computational science and social science ideas and approaches. Look forward to seeing the results and taking work forward.
- Fascinating, thought-provoking, exciting event. Very productive. Thanks!

This page left intentionally blank.

APPENDIX I: ACRONYMS AND ABBREVIATIONS

ColoRS	US-UK Collaboration on Resiliency and Security
CSD	DHS S&T Cyber Security Division
DHS	US Department of Homeland Security
MIT	Massachusetts Institute of Technology
NASDAQ	National Association of Securities Dealers Automated Quotations
PNNL	Pacific Northwest National Laboratory
S&T	DHS Science and Technology Directorate
STFC	UK Science and Technology Facilities Council

2014 U.S.–U.K. Program on Collaboration on Resiliency and Security (ColoRS) Working Meeting

Science & Technology Facilities Council

Homeland Security
Science and Technology