THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION
AND
HOMELAND SECURITY

MAY 2014
INTERNATIONAL

VOLUME 12 NUMBER 11

Click here to subscribe. Visit us online for this and other issues at http://cip.gmu.edu

Follow us on Twitter here
Like us on Facebook here

This month, *The CIP Report* presents its annual **International** issue. Recognizing that threats to critical infrastructure do not respect national boundaries, particularly in light of increasing global dependencies and interdependencies, our authors examine several foreign security and resilience approaches, as well as international partnership efforts.

GEORGE MASON UNIVERSITY
School of Law
CENTER for INFRASTRUCTURE PROTECTION and HOMELAND SECURITY

First, Eric Luiijf and Erich Rome examine the European Union's Critical Infrastructure Preparedness and Resilience Research Network, or CIPRNet. Dr. Katri Pynnöniemi then describes Russian efforts to secure critical infrastructure, and Drs. James Bohland, Paul Knox, and Jack Harrald introduce Virginia Tech's Global Forum on Urban and Regional Resilience, an initiative designed to facilitate international dialogue, multi-disciplinary research, and trans-disciplinary education and training. Next, Naouma Kourti, Adam Lewis, and David Ward present the European Reference Network for Critical Infrastructure Protection. Finally, Meghan Stepanek, Director of Baltimore's Office of Public Health Preparedness and Response, observes the need for grassroots efforts to build global networks necessary for addressing climate change.

We would like to take this opportunity to thank this month's contributors. We truly appreciate your valuable insight.

As always, we hope you enjoy this issue of *The CIP Report* and find it useful and informative. Thank you for your support and feedback.

Mick Kicklighter
Director, CIP/HS
George Mason University, School of Law

CIPRNet: EU's Network of Excellence for Resilient Critical Infrastructures

by Eric Luiijf, MS.c.* and Erich Rome, Ph.D.**

With co-funding by the European Union (EU), a European consortium works towards the establishment of a European Infrastructures Simulation & Analysis Center (EISAC). For Europe, the EISAC shall deliver Critical Infrastructure Protection (CIP) related services for Europe like those delivered by the National Infrastructure Simulation and Analysis Center (NISAC) in the United States and the Critical Infrastructure Program for Modelling and Analysis (CIPMA) in Australia.

The Critical Infrastructure Preparedness and Resilience Research Network (CIPRNet) project started on March 1, 2013. This Network of Excellence project is co-funded by the security research program within EU's 7th Research Framework Program (FP7). The CIPRNet consortium comprises six European research institutes (Fraunhofer, ENEA, TNO, CEA, JRC, Deltares), the international union of railways UIC, the universities of Rome, Cyprus, Bydgoszcz (Poland), and British Columbia (Canada), and ACRIS GmbH (Switzerland). The project coordination is by the German Fraunhofer Institute for Intelligent Analysis and Information Systems. The consortium brings together a unique set of knowledge and technology gathered in over sixty previous national and international research and development projects in the CIP field. Each consortium partner also functions as a multiplier by connecting their (inter)national networks and research platforms to CIPRNet's core activities and capabilities.

Within its lifetime of four years, the CIPRNet consortium will make a decisive effort towards providing support from the CIP research communities to emergency responders, government agencies, and policymakers, enhancing their preparedness and response capabilities regarding service disruptions in Europe's complex system of interconnected and dependent critical infrastructures (CI) across the 28 EU member nations and some associated nations.[1]

The expected long-lasting outcome of CIPRNet is an established multi-national operating EISAC with several nodes across Europe delivering CIP simulation, analysis, training, and other support services to national and regional emergency management centers as well as critical infrastructure operators. At the same time, the EISAC will maintain a collective knowledge and technology base on CIP and CI models and data, as well as be a focal point in European CIP research and development.

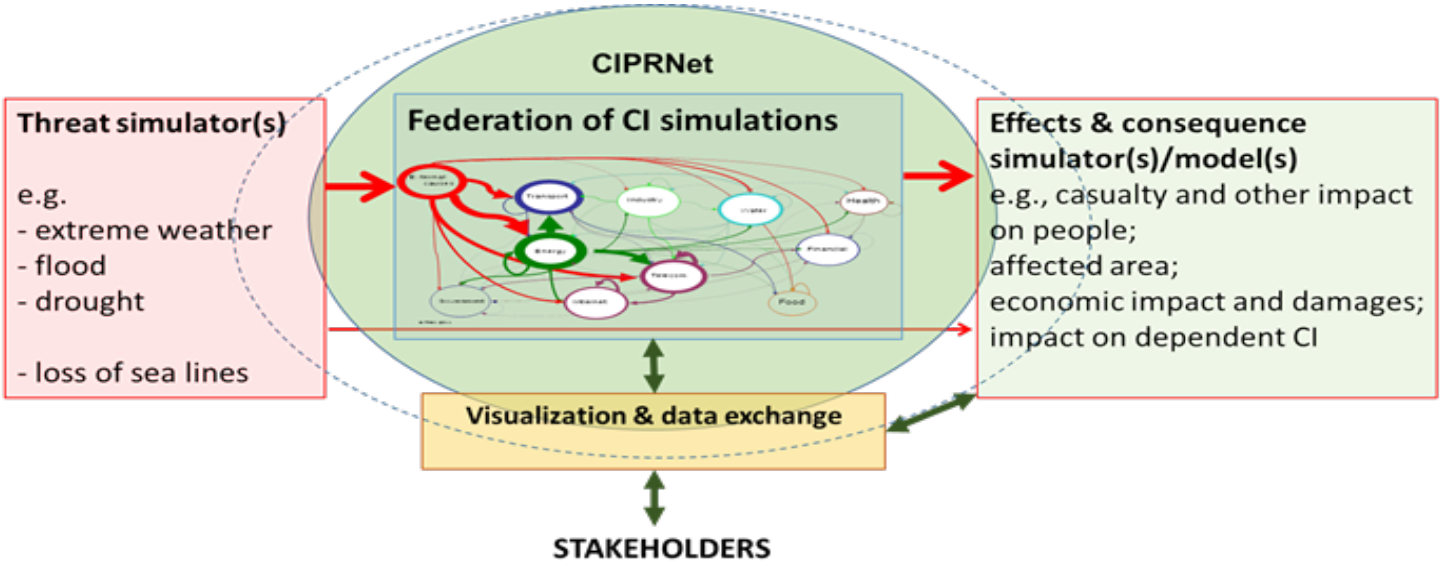
The CIPRNet Community

From the start, CIPRNet has involved its stakeholders in the design of the new capabilities. This is accomplished both by an International Advisory Board of end users and other stakeholders, and by the organization of targeted workshops and training events. The International Advisory Board currently has ten members from civil protection authorities, ministries, industry, and associations

(Continued on Page 3)

[1] The need for better understanding and preparedness is outlined in, H.A.M. Luiijf and M.H.A. Klaver, "Expand the Crisis? Neglect Critical Infrastructure! (Insufficient Situational Awareness about Critical Infrastructure by Emergency Management— Insights and Recommendations)" in: *Tagungsband 61. Jahresfachtagung der Vereinigung des Deutschen Brandschutzes e.V.*, 27-29.05.2013 (Weimar, Germany, 2013), pp. 293-304.

Figure 1: Positioning of CIPRNet



(Continued from Page 2)

fostering security and CIP. An Independent Ethics Board of experts in data protection and privacy ensures project results comply with legal and ethical standards. Moreover, any research group that can bring added-value to CIPRNet (and by that to their own progress) is welcome to connect to the network. Exchanges with other EU co-sponsored projects such as PREDICT (dependencies) and INTACT (extreme weather) are planned for.

New Capabilities

Reaching and maintaining the required level of CIP preparedness and responsiveness requires adequate and fast adaptation to on-going changes of CI. CIPRNet will implement advanced modelling, simulation, and analysis (MS&A) capabilities for supporting more effective responses to emergencies that affect or originate from multiple, dependent CI (see Figure 1). In particular, CIPRNet will create value-added decision support capabilities for national and multi-national emergency management. These capabilities will enable decision-makers and operators to analyze the various possible courses of action, to perform what-if analysis, and to learn about short and long term consequences of their decisions.

Apart from the core set of federated and interacting CI models, the threat side will comprise extreme weather threat models, flood models, and models of other threats that may affect multiple CI directly or through cascading effects. The effects and consequences analysis part will be based on real-time and statistical data, economic and other simulations and models, meteorological data, and more. The development of this new decision support capability will build upon pooling and integrating technologies and resources available though CIPRNet's partners and beyond. As an additional capability, CIPRNet plans to support the secure design of Next Generation Infrastructures like Smart Grids. The development of the new capabilities follows a model-based systems design approach. Key elements of this approach are scenario orientation, requirements engineering, and use cases.

Scenarios & Architecture

CIPRNet creates scenarios at different scales for developing, testing, and training the new capabilities. For instance, a regional scenario in one EU Member State will consider several dependent CI affected by threats like floods, landslides, and earthquakes. A scenario in a densely populated border region between two other Member States will consider a combination of

(Continued on Page 4)

(Continued from Page 3)

cross-border emergencies such as a dike breach affecting local CI with major cross-border impact.

International Capacity Building

In order to provide long lasting support from research communities, CIPRNet also aims at building required capacities. Numerous dissemination and training activities will contribute to this aim, including but not limited to the following:

- Dedicated cooperation workshops with other projects and networks in the field will contribute to increased coherence in the distributed multi-stakeholder community of CIP researchers and experts.

- Dedicated training activities will familiarize experts and potential end users with CIPRNet technology and knowledge. For example, at the end of April 2014, a first training session with over forty attendees took place in Paris.

- Young researchers will be trained via staff exchange between CIPRNet partners and by integrating CIPRNet lectures into the postgraduate Master in Homeland Security course at the Università Campus Bio-Medico in Rome, Italy. The next course will take place in July 2014. The planning for the 2015 sessions is in progress. Announcements and details regarding the training sessions can be found on the CIPRNet website.

- Apart from these external activities, the consortium partners exchange personnel to work on dedicated CIP and MS&A issues.

As outreach, the CIPRNet website contains information on the project, the events, and the ECN—the European equivalent of *The CIP Report*—a magazine on European CIP developments. The website will be extended over time with content and new functions such as:

- CIPedia ™—a wiki with many CIP-related resources, definitions, as well as debates to support CIP practitioners, policymakers, and CI operators.

- Ask-the-CIP-expert ™—a function to access practical CIP knowledge, CIP researchers, MS&A experts, etc., as well as to locate CIP best practices and resources (mainly in Europe).

- A CIP expertise database offering valuable knowledge and resources for stakeholders.

VCCC and EISAC

In order to achieve long-term impact and improvement, the new capabilities need to be consolidated and sustained beyond the duration of the CIPRNet project. For the development, consolidation, and dissemination of the new capabilities, CIPRNet will establish a virtual center of competence and expertise in CIP, the VCCC. The VCCC is a virtual facility, and during the term of CIPRNet will neither be a legal body nor a built structure. It will serve as a foundation for a European Infrastructures Simulation & Analysis Centre (EISAC), with the ultimate goal of sustaining the new capabilities and further innovations beyond the duration of CIPRNet.

A design study of the EISAC is available from the earlier completed, EU co-funded project, Design of an Interoperable European federated Simulation network for critical InfraStructures (DIESIS).[2] This design study will be employed in CIPRNet in the establishment of the VCCC and later the EISAC. The purpose is to found autonomous national EISAC nodes in Member States that will provide services tailored to the needs of the Member States. A central roof organization at a European level will ensure standardization of basic technology like middleware and modelling approaches, broker bilateral cooperation of EISAC nodes, and provide support at the EU

(Continued on Page 5)

[2] Uwe Beyer et al, Design of an Interoperable European federated Simulation network for critical InfraStructures (DIESIS): D4.1b Final Architectural Design (Sankt Augustin, 2010). Accessed April 30, 2014, www.diesis-project.eu.

(Continued from Page 4)
level.

Since transfer of research results into application and MS&A-based new decision support capabilities will be the focus of EISAC, it will complement the services of networks like the Critical Infrastructure Warning Information Network (CIWIN) and the European Reference Network for Critical Infrastructure Protection (ERNCIP).[3]

If interested in CIPRNet, please visit the website, take part in the events, or contact the authors of this article.❖

Acknowledgments

This article was written by the FP7 Network of Excellence CIPRNet, which is being partly funded by the European Commission under grant number FP7-312450-CIPRNet. The European Commission's support is gratefully acknowledged. Moreover, the authors gratefully acknowledge the contributions of their CIPRNet partners to this article. It should be regarded as a joint publication of the consortium. The content of this publication does not reflect the official opinion of the European Union. Responsibility for the information and views expressed therein lies entirely with the authors.

**Eric Luiijf, M.Sc.*

Eric Luiijf is principal consultant at the Netherlands Organisation for Applied Scientific Research TNO. As expert he has contributed to many national and EU projects in the field on Critical (Information) Infrastructure Protection, both at the technical and policy levels, since 2000. Eric has published many popular articles, reports, and peer-reviewed publications about cyber terrorism, C(I)IP, process control security, information assurance, and cyber operations. He has been interviewed many times by press, radio and TV on these topics.

***Erich Rome, Ph.D.*

Erich Rome is a senior researcher and project manager at Fraunhofer-Institut für Intelligente Analyse und Informationssysteme IAIS' ART department in Germany. Since 2007, Erich Rome has investigated MS&A for CIP and multi-sensory systems for surveillance and security. He has published numerous peer-reviewed publications, edited several books, and is a member of the steering committee of the workshop series CRITIS. To date, he has coordinated four EU projects, CIPRNet being the current one.

[3] See *infra*, p. 13, for further discussion of the European Reference Network for Critical Infrastructure Protection.

Problematization of Critical Infrastructures in the Framework of Russian National Security

by Katri Pynnöniemi, Ph.D., Senior Research Fellow,
The Finnish Institute of International Affairs

The current Russian policy on critical infrastructure protection (CIP) was outlined in the early 2000's and has been consolidated in recent years as part of the national security strategy. The Russian policy resembles those outlined in the United States and Europe, yet the way in which the key ideas presented in the policy 'hang together' reveals underlying differences in the policy fields.

One of the key differences is the articulation of the 'critical infrastructures' in the public discourse. The basic problem of CIP in Russia is expressed with reference to 'over 45,000 potentially dangerous objects located in the country and over 90 million people living in high-risk zones.'[1] However, the notion of CIP is rarely used in the Russian media or policy documents. Instead, this phenomenon is discussed using various other terms, such as 'strategic object' (*strategicheskii obj'ekt*), 'dangerous industrial object' (*opasnyi proizvodstvenniyi ob'ekt*), 'very important object' (*osobo vazhnyi ob'ekt*), 'very dangerous technically complex object' (*osobo opasnyi i tehnicheski slozhnii ob'ekt*), and 'potentially dangerous objects.'[2] These terms are used interchangeably with the concept of 'critically important objects' (*kriticheski vazhnyh ob'ektov, KVO*). Underlying this terminology is the categorization of these objects in accordance with risk scales and zones. Yet, problematization of *interdependency* as the main risk of the critical infrastructure is rarely voiced in the Russian context. Russian researchers have pointed out that lower level of automatization in the Russian industry can partly explain this difference to general discussion in the United States and Europe.

The second key difference relates to the way in which the critical infrastructures were identified as a policy problem in the first place. In the 1990's and early 2000's, Russia's policy on CIP was framed predominantly as an aspect of environmental and technological security, with the Chernobyl disaster in 1986 playing a major role in the Russian expert discussion. The joint session of the Security Council and the State Council in November 2003 can be considered as the starting point for the re-formulation of the current Russian policy on CIP. In his opening statement at this meeting, President Vladimir Putin emphasized that the protection of critical infrastructure to national security objects from man-triggered, nature-generated or terrorist threats is an acute task and requires the joint action of the state authorities and economic organisms. Putin explained that the new policy is required because Russia's run-down infrastructures are prone to malfunction, and the risk of man-triggered catastrophes is further aggravated due to widespread indifference to safety rules and norms. In addition, each year more and more natural catastrophes such as hurricanes, earthquakes, and forest fires are reported in Russia.[3]

(Continued on Page 7)

[1] P. Tsalikov, V.A. Akimov, and K. A. Kozlov, *Otsenka prirodnoi, tehnogennoi i teknologicheskoi besopasnosti Rossii* [Analysis of natural, technical and technological security of Russia], FGU VNII GOTcS, MChS Rossii, (2009); President of RF, *Osnovy gosudarstvennoi politiki v oblasti obespecheniya besopasnosti naseleniya RF i zashchishchennosti kriticheski vazhnyh i potentsialno opasnyh ob'ektov ot ugroz prirodnogo, tehnogennogo kharakteri i terroristicheskih aktov na period do 2020 goda* [Foundations of state policy on the protection of population and critical infrastructure from natural catastrophes, technological disasters and terrorist acts until 2020], No. Pr-3400 (15 November 2011).

[2] The analysis is based on a search that was conducted through the Integrum search engine and listed articles that appeared in major federal newspapers in Russia between 2000 and 2010.

[3] Vladimir Putin, "Vstupitel'noe slovo na sovmestnom zasedanii Soveta Bezopasnosti i preziduma Gosudarsvennogo soveta po voprosu o povyshenii zashchity kriticheski vazhnyh dlya natsional'noi bezopasnosti ob'ektov infrastruktury i naseleniya strany v usloviyah obostreniya ugroz prirodnogo, tehnogennogo, i terroristicheskogo haraktera," (13 November 2003) http://archive.kremlin.ru/text/appears/2003/11/55532.shtml.

(Continued from Page 6)

A study published in 2011 gives an idea of the scale of this problem. According to this study, approximately 70 percent of all disasters occurring in Russia are technological accidents and catastrophes. Furthermore, the study found that the "most frequent among all technological accidents and disasters triggered by natural hazardous events (Natechs) are breakdowns in electric power supply systems."[4] One of the latest major emergency situations, the flooding in the Russian Far East in September 2013, is estimated to have cost over 500 billion rubles for the economy and society as a whole.[5] In 2003, Putin argued that in order to tackle these problems, state policy must be reshaped.[6]

Although the 2003 meeting of the Russian Security Council was characterized as the 'defining moment' for the elaboration of CIP policy in Russia, certain steps in this direction were already taken in the late 1990's. The first government programme 'on the reduction of risks and moderation of the consequences of emergency situations caused by natural or man-triggered disasters in the Russian Federation until 2005' was approved in September 1999. It outlines the basic principles and objectives for the establishment of a unified state system of disaster warning and relief.[7]

The emphasis put on the development of risk management capabilities has been consistent over the years. In the latest federal level programme from 2011, the ambition is to develop a scientific-methodological basis for risk management, and a set of "long-term strategies and organizational-financial mechanisms" that enhance the interaction, coordination, and targeting of resources for the purposes of catastrophe and emergency prevention.[8] The purpose is to improve the monitoring and forecasting capacities to the extent that they cover 80 percent of technology- and nature-generated risks.[9] A new culture of emergency response is also required to achieve this objective. This new culture is one of "informing and alerting about emergency situations," which in turn, is formed on the basis of next-generation systems of emergency situation monitoring and forecasting, wider use of new information technologies for these purposes, and the implementation of a system of measures for ensuring the comprehensive security of population and territory by 2015.[10]

During the last twenty years, administrative and financial resources for emergency prevention have been consolidated under the Ministry of Emergency Situations of Russia. The Ministry was formed on the basis of the Russian civil-military agency (MO RSFSR) in July 1991. The first head of the agency (and later Ministry) was Sergei Shoigu, who served in this position until May 2012 when he became a governor of Moscow region.[11] Today,

(Continued on Page 8)

---

[4] Elena Petrova, "Critical Infrastructure in Russia: Geographical Analysis of Accidents Triggered by Natural Hazards," *Environmental Engineering and Management Journal*, vol. 10, no. 1 (2011): 58.

[5] Pravitelstvo RF, *O sotsial'no-ekonomitseskom razvitii Dalne'go Vostoka* [Government meeting on the social-economic development of the Far Eastern Region of Russia] (25.4.2014) http://government.ru/news/12006#trut; Discussion with expert from Emercom of Russia, Center for Strategic Research of Civil Defence, 17.04.2014, Moscow, Russia. Authors notes.

[6] Vladimir Putin, "Vstupitel'noe slovo na sovmestnom zasedanii Soveta Bezopasnosti i preziduma Gosudarsvennogo soveta po voprosu o povyshenii zashchity kriticheski vazhnyh dlya natsional'noi bezopasnosti ob'ektov infrastruktury i naseleniya strany v usloviyah obostreniya ugroz prirodnogo, tehnogennogo, i terroristicheskogo haraktera," [Opening remarks at the joint meeting of the Security Council and the Presidium of State Council on protection of objects of infrastructure critical to national security and population in acute threats of natural, man-triggered and terrorist character] (13 November 2003) http://archive.kremlin.ru/text/appears/2003/11/55532.shtml

[7] Postanovlenie Pravitelstvo RF, *O federalnoi tselevoi programme 'Snizhenie riskov i smyagchenie posledstvii chrezvytsainyh situatsii prirodnogo i tehnogennogo kharaktera v RF do 2005 goda* [On the federal programme 'On the reduction of risks and moderation of the consequences of emergency situations caused by natural or man-triggered disasters in the RF until 2005'], No. 1098 (29 September 1999).

[8] Postanovlenie Pravitelstvo RF, *O federal'noi tselevoi programme "Snizhenie riskov i smyagchenie posledstvii chrezvychainyh situatiprirodnogo i tehnogennogo haraktera v RF do 2015 goda* [On the federal programme 'On the reduction of risks and moderation of the consequences of emergency situations caused by natural or man-triggered disasters in the RF until 2015'] No. 555 (7 July 2011): 13.

[9] Ibid.

[10] Ibid. After the Moscow metro bombing on 29 March 2010, President Medvedev ordered the establishment of a new monitoring system for public transport in Moscow and other cities by 2014. President Rossii, *O sozdanii kompleksnoi sistemy obespecheniya bezopasnosti naseleniya na transporte* [On the establishment of complex security system of public transport] (31 March 2010) http://news.kremlin.ru/news/7295/print.

(Continued from Page 7)

the Ministry has over 200,000 employees, responsible for international and domestic rescue services and civil mobilization in Russia. The creation of the National Crisis Management Center[12] in 2006 and the establishment of the risk analysis department within the Federal Science and High Technology Centre in 2009 also point towards prioritization of a risk management policy.

Parallel to this policy, critical infrastructures have been problematized as an issue of state and public security. The latest National Security Strategy of 2009 addresses the issue of terrorism vis-à-vis critical infrastructures:

The activity of terrorist organizations, groups and individuals that aim at the disruption of the normal functioning of state bodies, or the destruction of military or industrial sites, enterprises and institutions providing vital social services, and the intimidation of the population by means including nuclear and chemical weapons or dangerous radioactive, chemical and biological substances.[13]

In contrast to most definitions of critical infrastructure, the text does not make reference to the cyber sphere and the interconnectivity of complex systems as points of vulnerability. Also noticeable in the document is the emphasis on the protection of *way of life*—consisting of broad tasks such as 'healthy lifestyle,' food security, high quality medicine, and healthcare.[14] This reflects the general notion in Russia whereby the country is no longer portrayed as a 'weak state,' but is said to have "overcome the consequences of the systemic socio-political and economic crisis of the end of the 20th Century."[15]

When analysing the multiple policy documents on CIP, it is worth noting that they evolve against a background comprised of an uneasy combination of factors: the degeneration of infrastructures critical for the country's economic and social development, and closing from public foresight the institutions responsible for protecting population and territory. The first factor is widely acknowledged and the lack of real investments to infrastructure development (and maintenance) is generally believed to result from systematic corruption and short-sighted decision-making, both among business and political elites. Russian power-structures responsible for public safety and security are effectively managing the public space and increasingly suppressing voices critical to authorities. Although both of these factors have been articulated in the Russian discussion, they are not often linked, at least in the political discourse, with the ability of the country to cope with multiplying natural emergencies and technological disasters. Discussions within the Russian expert community are, however, encouraging regarding the multiple challenges ahead.❖

[11] On November 6, 2012 President Putin replaced Defence Minister Anatoly Serdyukov and appointed Shoigu to this post.
[12] EMERCOM, 'National Crisis Management Center,' http://www.mchs.gov.ru/eng/powers/?SECTION_ID=609.
[13] *National Security Strategy of Russia, approved by Presidential decree No. 537* (12 May 2009).
[14] Ibid.
[15] Ibid.

New Resilience Organization at Virginia Tech

by James Bohland, Ph.D., Co-Director; Paul Knox, Ph.D., Co-Director;
and Jack Harrald, Ph.D., Assistant Director,
Global Forum on Urban and Regional Resilience, Virginia Tech – Arlington

The Global Forum on Urban and Regional Resilience (GFURR) is a presidential initiative at Virginia Tech, established in 2013 to build on the expertise of existing faculty to advance resilience research and practice at the university and in the broader community. GFURR brings together faculty from Virginia Tech and partner organizations to expand the knowledge base on the resilience of places and regions. Resilience has become an important concept in planning and policy in response to vulnerabilities resulting from a variety of forces, including climate change, economic, social and political instability, and rapid urbanization. As a result, the scientific literature on resilience has seen remarkable growth in the past five years as the concept has gained credence and become part of the lexicon of policymakers around the world. Local, national, and global organizations have established programs to recognize resilience, created metrics to measure aspects of resilience, and adopted policies intended to enhance resilience. All of this has occurred within a multi-disciplinary, multi-scale matrix that has helped accelerate the diffusion of the concept of resilience; but that also has created confusion about definitions and approaches, leading to critiques of what some consider a nebulous idea.

Research and application of resilience concepts tend to have been organized within individual intellectual domains such as engineering, ecology, social ecological systems, and neurology. Consequently, definitions and use of the concept are labeled as engineering resilience, ecological resilience, socio-ecological-systems, or disaster resilience, for example.[1] At best, the multitude of definitions requires every author to clarify the specific nature of their use of resilience, while at worse it creates confusion as scholars and decision-makers talk across one another on how the concept can be useful. One important GFURR aspiration is to bring some clarity to the conceptual framework of resilience as it is pertains to different intellectual domains. The aim is to explore new and innovative ways of increasing the utility of the concept as both an analytical lens and as a policy framework for advancing the social wellbeing of places. GFURR views resilience as a system-of-systems concept. Systems confront change in multiple ways—resisting, rebounding, adapting, or transforming. Understanding how a complex system such as a city responds to external forces requires the integration of physical, social, and behavioral perspectives. GFURR will contribute to this by:

- Facilitating global conversations among scholars and practitioners with significantly different perspectives and responsibilities through co-sponsorship of workshops and conferences designed to explore key conceptual and methodological issues
- Facilitating multi-disciplinary research on under- and unexplored dimensions of resilience
- Encouraging the establishment of trans-disciplinary educational and training curricula to ensure that future practitioners and researchers have a wide-reaching viewpoint of resilience
- Connecting research and practitioner communities through the establishment of living lab environments in both urban and rural settings.

(Continued on Page 10)

[1] For reviews of resilience definitions see P. Martin-Breen and J. Marty Anderies, *Resilience: A Literature Review,* New York: The Rockefeller Foundation, 2011; Mark Scott, "Resilience: A Conceptual Lens for Rural Studies," *Geography Compass*, 7 (2013): 597-610; or Carl Folke, et al., "Resilience Thinking: Integrating Resilience, Adaptability and Transformability," *Ecology and Society*, 15 (2010): 4.

(Continued from Page 9)

GFURR facilitates a global conversation through sponsorship of workshops and conferences that bring together researchers, practitioners, and policymakers with divergent perspectives. Since 2010 GFURR or its antecedent, the Center for Community Security and Resilience, have sponsored four international conferences either in Switzerland (Zurich and Davos) or in the Washington DC area. A workshop on use of urban informatics to support urban resilience and a conference on ethical and normative aspects of resilience are scheduled for 2014. The convening of scholars and practitioners is also being achieved by partnering with a number of organizations that address resilience in some fashion. At present these include:

- Global Risk Forum, Davos, Switzerland
- National Academy of Science Roundtable on Risk, Resilience, and Extreme Events, Washington, DC
- Meridian Institute, Washington, DC
- Social and Decision Analytics Lab at the Virginia Bioinformatics Institute
- Chesapeake Crescent Initiative, National Capital Region
- UDEL Disaster Research Center, Wilmington, DE

Climate change and the resultant acceleration of the incidence of extreme weather events, together with global forces that challenge national and regional economies, rapid urbanization in much of the world, and increased social volatility fostered by economic disparities, religious conflict, and political unrest create conditions that require cities and regions to become more innovative in maintaining quality of life for their citizens. GFURR is particularly interested in research on how resiliency-oriented policies and practices may enhance or detract from people's wellbeing. To that end, GFURR believes that research should address the following five questions:

1. What are the normative and ethical issues associated with creating and maintaining resilient environments?

Policies to enhance resilience will inevitably favor some groups or regions over others. Who makes those decisions, and the subsequent impacts on cities and regions from those decisions are vital research issues for the future.

2. What are the major barriers to creating socially equitable and resilient places?

Despite the increased awareness of resilience as a planning concept, progress towards achieving more resilient places meets with resistance by some groups, political leaders, and citizens. Becoming more resilient is difficult to oppose in theory, but when implementation challenges a national ethos or requires public financial commitments, opposition occurs. Understanding barriers to achieving resilience is essential to effective policy development.

3. How might new analytics and informatics contribute to understanding the resilience of places?

The rapid expansion of social media and the "internet of things" offer interesting opportunities for empirically analyzing different dimensions of systems not previously possible. To do so, however, requires analytical systems capable of integrating disparate data formats, managing and analyzing large volumes of data in useful time frames, and presenting information in ways that are useful and transparent to citizens and policymakers alike. GFURR supports efforts in exploring new analytic approaches in resilience research.

4. In what ways do the interaction of physical and socio-technical systems require system adaptation or transformation to maintain the wellbeing of a place and its citizens?

Prior research in ecology or social-environment systems (SES) stresses the adaptive or transformational necessity for eco-systems to survive major disruptive forces.[2] Similarly, research on the social consequences of environmental- techno disasters such as Exxon Valdez, Katrina, or Fukushima reveal significant social and welfare impacts from changing the existing interdependencies in the complex physical and socio-

(Continued on Page 11)

[2] See Nicholas Gotts, "Resilience, Panarchy, and World-Systems Analysis," *Ecology and Science*, 12 (2007): 24; S. Wilson, et al., "Separating Adaptive Maintenance (Resilience) and Transformative Capacity of Social-Ecological Systems," *Ecology and Science*, 18 (2013): 22.

(Continued from Page 10)

technical synergies that defined local and regional societies prior to the disasters. GFURR encourages research that analyzes the adaptive and transformational processes and that assesses the consequences of those interactions on the wellbeing of places and citizens.

5. What are the appropriate roles for government, non-profits, and the private sector in constructing socially equitable and resilient places?

The technical, social, and financial requirements for constructing resilient places cannot be achieved unless all sectors of society work jointly. The fiscal and social costs are too great for governments—federal, state, or local. Partnerships across sectors must be achieved; however, best practices for achieving successful partnerships still must be researched and implemented. GFURR has established collaborative financing and programming as a critical area for investment of its research resources.

GFURR is assisting faculty at Virginia Tech to develop graduate programs, degrees, and certifications that integrate knowledge from different disciplines. The goal is not simply to bring multiple voices to bear on the concept of resilience, but to create "concept-based" learning, what we term trans-disciplinary learning, that generates knowledge by focusing multiple disciplines on a specific concept and using new insights gained by that approach to inform traditional disciplines. A key component of this trans-disciplinary approach is to transition knowledge to practice effectively. Drawing from Virginia Tech's land grant tradition, GFURR is helping to establish a "living lab" approach to graduate education. The living lab concept brings together researchers, students, and practitioners in an environment where mutual learning occurs. The problems of the practitioners establish pathways to new research and subsequently to new solutions for practitioners and new curricula for students. The living lab becomes the teaching and research "hospital" for resilience where students and researchers solve the challenges facing urban and regional policymakers.

The Global Forum for Urban and Regional Resilience is currently led by Dr. Paul Knox, co-director; Dr. James Bohland, co-director; and Dr. Jack Harrald, associate director, located in the Virginia Tech Research Center— Arlington. Per its mission to create knowledge through partnering and collaborative efforts, GFURR welcomes opportunities to work with other organizations interested in advancing our understanding of resilience and in helping our cities and regions build societies that enhance the wellbeing of all citizens through thoughtful and innovative policies.❖

More information on the Forum can be found at www.gfurr.vt.edu. We welcome those interested in helping the Forum achieve its goals. Please contact us at gfurr@vt.edu.

The Global Forum on Urban and Regional Resilience at Virginia Tech announces new conference series: "New Perspectives on Resilience"

This conference series builds on the Community Resilience series begun in 2010 and reflects GFURR's broader mission to understand regional and urban resilience globally within a trans-disciplinary context.

Inaugural Conference: "Normative Aspects of Resilience"
October 12-14, 2014

For more information, including registration, Call for Papers, and draft agenda, please visit www.gfurr.vt.edu

Global Forum on Urban and Regional Resilience

Progress and Achievements of the European Reference Network for Critical Infrastructure Protection

by Naouma Kourti,* Adam Lewis, and David Ward

In 2008 the European Commission (EC) organized a network of research and technology organizations within the European Union (EU) with capabilities in critical infrastructure protection (CIP), called the European Reference Network for Critical Infrastructure Protection (ERNCIP). An in-depth preparatory study was carried out in 2009–2010 by the EC's Joint Research Centre (JRC) on behalf of the Directorate-General for Home Affairs ("DG HOME"). A JRC task force assessed the requirements of the proposed network and concluded that its members should be research and technology organizations within the EU with the expertise, experience, facilities, and equipment to work on the technical aspects of CIP. It should be devoted to experimental security, methods and standards for testing and performance evaluation, studies in preparation for threat and risk assessment, and understanding CI dependencies. It should be designed to meet the priorities of the EC, Member States' (MS) governments and CI stakeholders and be coherent with EU CIP policy in general. ERNCIP should help the MS to supplement their national technical capabilities. The mission would be:

"To foster the emergence of innovative, qualified, efficient, competitive security solutions, through networking of European experimental capabilities."

This preparatory work resulted in a four year roadmap and a proposal to develop an on-line inventory of CIP laboratory and testing facilities and thematic groups to tackle specific CIP thematic areas. The proposal was endorsed in late 2010 and the ERNCIP project entered its implementation phase in early 2011.

T0-T12	**Core Functionalities:** Development of inventory database and setting-up of Thematic Groups (TGs)
T12-T24	**Initial Operations:** Launch of inventory database and start of TG initial operations and reporting
T24-T36	**Knowledge Exploitation:** TG continuation and dissemination of findings
T36-T48	**Consolidation:** TG continuation and recommendations and proposal for ERNCIP2

In ERNCIP's first two years, work has been dedicated to setting up the core functionalities of the network, i.e. the searchable database and the thematic groups (TGs). The current database has over 100 registered facilities, representing 20 MS with traffic currently running at 50 searches per month. There are now eight TGs in operation, namely:

(Continued on Page 13)

Current Thematic Area-Group Title	Lead Organization and Background
1. Aviation Security Detection Equipment (AVSEC)	JRC-IRMM (Geel, Belgium). In close cooperation with the European Commission this group is focusing on common test methodologies for Scanners, and Detection Systems.
2. Explosives Detection Equipment (non-Aviation) (DEMON)	CEA – Le Ripault (France). DEMON works towards providing the initial elements for a European common testing methodology for explosives detection equipment based on the needs identified in the non-aviation sectors.
3. Industrial Automatic Control Systems and Smart Grids (IASC&SG)	TNO (The Netherlands) and Thales Group (France). There are many existing and previous activities that cover this thematic area. This TG therefore is seeking to take all these initiatives into account and build on the results already achieved.
4. Resistance of Structures against Explosion Effects	Fraunhofer EMI (Germany). The resistance of civil buildings against explosive attacks is a relatively new area. Today the regulations available are very limited, and, consequently, there is no harmonized system of testing.
5. Chemical & Biological Risks in the Water Sector	Austrian Environmental Agency. The harmonization and definition of testing methodologies of innovative real-time alarm systems to prevent or mitigate drinking water contamination.
6. Video Analytics and Surveillance	CAST (UK). Closed-circuit TV (CCTV) cameras are increasingly used in the protection of CI. While new methods are emerging for surveillance and image analysis it is becoming more crucial to harmonize methodologies for the testing and evaluation of these new technologies.
7. Applied Biometrics for CIP	CAST (UK). This group focuses on Automated Border Controls, physical access control, logical access control, mobile identity checks, and biometric recognition of individuals from CCTV.
8. Radiological Threats to Critical Infrastructure	STUK (Finland). This group was set-up in April 2013 and focuses on three tasks: list-mode data acquisition based on digital electronics, remote expert support of field teams, and remote controlled radiation measurements and sampling using unmanned vehicles.

(Continued from Page 12)

The inventory and TGs are managed by the ERNCIP office that acts on behalf of the EC, MS, and stakeholders. The current ERNCIP organization structure is three-tier: 1) EC and MS, 2) Advisory bodies and ERNCIP Office, and 3)TGs and relevant coordinators.

Creating such a network implies building a community based on trust, where knowledge can be shared amongst members. Unsurprisingly, the organizations' representatives first sought to understand the potential of the database and TG work before committing. Knowledge was shared providing there was benefit in doing so and that sufficient controls were in place. This required adequate formal governance, including common terms of reference, acceptance of membership agreements, and a protocol to securely share any data, information, or knowledge.

Once the relationship between actors and relevant boundaries had been established, the next level of cooperation was based on more informal and mutual trust. CIP experts in each thematic area were brought together, often for the first time, despite the fact that the theme was well known and shared by the MS. Many issues had to be addressed in the TG work. The various organizations involved had differing business aims and different objectives: these could range from looking for funding to developing new de facto standards or defining test protocols. And the information that had to be exchanged was in some cases very sensitive.

This requires good relationships within and across policy and business domains. To this end, two dedicated ERNCIP conferences were organized, one with the theme of Trust and one for CIP Operators

(Continued on Page 14)

(Continued from Page 13)

dialogue.

A secure document repository was also created on the EC's CIRCABC platform to access and exchange information. Legal Advisory, Academic, and Expert Committees were also set up. A website, regular quarterly newsletters, and active participation at key CIP events help promote ERNCIP and further strengthen the community.

CIP security has been confirmed to be much more complex, cross-sectorial, and evolutionary than originally thought. It is not only technology and innovation driven but also interlaced with questions of insufficient or excessive policy, evolving or new threats, real-time or delayed event monitoring, etc. Indeed, while a CIP innovation might already be in the pipeline, or even available, there are other constraints, such as the leveraging of national standards as trade barriers, or the fragmentation of markets and product offerings.

It is also for this reason that the TGs have focused on both short and medium-long term deliverables. First, it demonstrates that real daily issues stressed by the operators are being tackled and second, that proper emphasis is placed on policy and legislation, without strangling the business arena.

A brief look at some of the TGs will show what is being produced.

The water sector already has well over 500 standards worldwide, so the water sector TG took care to focus on an unaddressed issue: harmonizing the testing methodologies of innovative real-time alarm systems for drinking water contamination. Today's organizational structures, scientific methods, and regulatory frameworks concerning drinking water quality are designed for long term decision making and not for immediate incident response. Tools have been recently developed to measure water quality in real-time. However, there are several factors which influence the performance of these tools, and there is no EU standard approach which sets out parameters for an overall assessment of water quality.

The work of this TG concentrates on:

1. The use of innovative probes, sensors, etc. and enabling technologies for online measurement of water quality in drinking water distribution networks.

2. Rapid identification and quantification of chemical and biological contaminations in drinking water.

3. Citizens' engagement and participation in sharing relevant observations.

The resistance of structures against explosion effects was already highlighted as a key theme in the preparatory phase of ERNCIP. The relevant TG confirmed that the explosion-resistance of civil buildings, and building elements, has only been considered in the last decade and is consequently only now being understood by governments and society. Few regulations are available and there is no harmonized testing system. While there is a lot of testing experience in individual facilities and laboratories, each facility has its own testing methods, and there are few published, harmonized experimental procedures. The same goes for dynamic numerical simulation methods where, in general, no regulations or accepted guidelines have been established. Consequently, the TG sought to develop guidelines to help to harmonize procedures in the testing of structural elements against explosion-induced loads. First, the loading characteristics of an external and an internal explosion are different. The focus is, for now, on external detonations only. Second, the TG is concentrating on far-field blast loading and the specification of the test methods to define the resistance of structural elements against it. Third, the plan is to start with an element for which a regulation is available: windows and glazing. Later, the same harmonization process will be applied to other structural elements.

The work of the TG on Aviation Security was aligned with the work program of the European Civil Aviation Conference (ECAC) Technical Task Force, which has a formal cooperation with the EC. The TG has performed independent validation of the testing methodologies used in ECAC's "Common Evaluation Process (CEP)", for certain critical types of detection equipment used in airports, as a step towards fully integrating the evaluation process into European

(Continued on Page 15)

(Continued from Page 14)

Aviation Security legislation. Reports have been issued on Explosive Trace Detection in EU Legislation and on Detection Requirements and Test Methodologies. The planned work of this TG is now complete, and can be taken up by the existing EU aviation security mechanisms. The need for new ERNCIP work in aviation is under review.

Examples of important non-aviation contexts addressed by the TG on Detection of Explosives Materials for Operational Needs (DEMON) are urban transport and large public events. The TG has issued a Statement of User Needs, based on a detailed examination of the members' experiences in these and other fields. In support of DEMON, the JRC has made a summary of relevant European legislation, which is publicly available on the ERNCIP website.

The TG on Radiation Detection Equipment, established only last year, is already close to completing a new draft data standard for "list-mode" radiation detectors, i.e. those with digital output. This was identified as a useful next step, following the completion of the Illicit Trafficking Radiation Assessment Program (ITRAP+10), a joint project between the EC and the US Department of Homeland Security (Domestic Nuclear Detection Office) to test radiation detectors. ITRAP+10 was, in January 2014, itself extended to a new phase.

It is expected that the current ERNCIP Project (ERNCIP1) will be concluded in the first quarter of 2015, so discussion for continuation is already underway, based on the following key underpinnings:

A. There is a need for a trusted environment when dealing with security issues, which takes time to establish, and it is only after this important foundation is in place that quality results can be expected. Once such an environment exists, it is worth preserving.

B. Issues dealt with within the TGs require significant efforts that go beyond ERNCIP's annual budget allocations.

C. The EU has only recently started to create its own security and CIP profile and there is still much work to do in preparing guidelines and harmonized test protocols as well as in identifying gaps and needs in testing.

A proposal for ERNCIP2 and a relevant strategy to 2020, has now been submitted to DG HOME, articulated around three areas:

1. Policy Context, including strategic goals and objectives

2. Roll-out and implementation

3. Financing, with a clear intent to enhance the community that has been successfully built.

In conclusion, ERNCIP is now producing output that contributes usefully to CIP, and there is a clear vision of how to continue to obtain benefits from the trusted environment that has been created. ❖

**For further information please contact Naouma Kourti, European Commission, Joint Research Centre, Institute for the Protection and Security of the Citizen, Security Technology Assessment Unit Via E. Fermi 2749, I-21027 Ispra (VA), Italy*

E-mail: erncip-office@jrc.ec.europa.eu
Website: http://ipsc.jrc.ec.europa.eu/index.php/ERNCIP/688/0/
Tel +39 0332 786045
Fax +39 0332 786565

Love in the Time of Climate Change: Inspiring Devotion in Global City Communities

by Meghan Stepanek, J.D., M.P.H.,
Director, Office of Public Health Preparedness and Response,
Baltimore City Health Department

On May 7, 2014, Christiana Figueres, the Executive Secretary of the United Nations Framework Convention on Climate Change (UNFCCC) gave a speech at St. Paul's Cathedral in London aimed at building will for action. She highlighted the overwhelming scientific data as well as the consequences of climate change already witnessed across the globe. While she pointed to many finance, technology, and policy solutions as demonstrations of leadership, Figueres emphasized love as the missing element in climate change to "build the courage, the confidence, the political space and urgency for accelerated action."[1] The array of individual efforts she cited, such as changes in dietary choices, transportation, electricity consumption, selection of carbon neutral goods/renewable energy sources, all focused on people taking grassroots actions to make a difference on a global scale. While community action holds significant promise for climate change mitigation and adaptation, galvanizing people for major changes is difficult without the strong appeal to human interests and without a clear sense of the impact. Undoubtedly, the challenges of addressing climate change are daunting, but grassroots-level action can be further developed by strengthening the ways in which community groups connect to and receive feedback from global networks to reinforce that their efforts are meaningful, interconnected, and make the kind of difference that merits devotion.

The United Nations Framework Convention on Climate Change (UNFCCC), Article 1, defines climate change as "a change of climate which is attributed directly or indirectly to human activity that alters the composition of the global atmosphere and which is in addition to natural climate variability observed over comparable time periods."[2] While the scientific evidence has grown stronger, as detailed in updated reports from the United Nations Intergovernmental Panel on Climate Change (IPCC),[3] and policy and planning efforts have flourished,[4] inspiring community actions at the local level, particularly in cities, is still an urgent need for change to be seen.

Many climate change mitigation and adaption strategies have focused on cities internationally as estimates suggest that urban areas are responsible for 75 percent of global carbon dioxide emissions.[5] With high population density, high use of transportation, and buildings producing greenhouse emissions, cities are not only contributing to climate change impacts, but are more vulnerable to the consequences such as extreme weather. City government officials have been called on to address global climate change by undertaking local action without widespread community support. Cities across the globe each face unique challenges in addressing climate change, but all share in the struggle to implement measurable and long-term changes with competing urgent priorities. The

(Continued on Page 17)

[1] Christiana Figueres, "Climate Change: Building the Will for Action." Speech, London, May 7, 2014, United Nations Framework Convention on Climate Change. https://unfccc.int/files/press/statements/application/pdf/20140705_stpaulslondon.pdf.

[2] United Nations Framework Convention on Climate Change, Article 1, "Definitions," March 21, 1994, http://unfccc.int/essential_background/convention/background/items/2536.php.

[3] Christopher B. Field, et al., "Climate Change 2014: Impacts, Adaptation and Vulnerability," Intergovernmental Panel on Climate Change (IPCC) WGII AR5 Summary for Policymakers, March 31, 2014, http://ipcc-wg2.gov/AR5/images/uploads/IPCC_WG2AR5_SPM_Approved.pdf.

[4] carbonn Cities Climate Registry , Chart of Data on 'Actions,' http://citiesclimateregistry.org/fileadmin/user_upload/Images/Actions.jpg. The largest portion of report activities are policy/strategies/action plans (44%) but the combination of education, organizational/governance, and public participation account for substantially less (16%).

[5] United Nations Environment Programme, "Cities and Climate Change," http://www.unep.org/resourceefficiency/Policy/ResourceEfficientCities/FocusAreas/CitiesandClimateChange/tabid/101665/Default.aspx, accessed May 19, 2014.

(Continued from Page 16)

complexity of climate change issues means that developing political will is hardest when the community is not able to clearly see the impact. With the breadth of issues that are involved in climate change, it is also hard to appeal to established community interests without dividing the various issues in a way that complicates leadership and tracking the impact.

Even while the context is challenging, international cities hold the greatest promise for major climate change action because they are well positioned to lead community engagement efforts. In recognition of the importance of global networking between cities tackling these issues, the World Mayors Council on Climate Change (WMCC) and the C40 Climate Change Group were both formed in 2005. The WMCC has brought together local governments in cooperation for advocacy. Additionally, the C40 Climate Leadership Group has provided a networking opportunity for the largest cities and coordinated analysis of the cities' mayoral powers in key areas related to climate change, monitored activities by initiatives (adaptation and water, energy, finance and economic development, measurement and planning, solid waste management, sustainable communities, and transportation), and provided data on the measurement of greenhouse gas emissions and climate risks.[6]

Cities' resource scarcity makes it hard to justify public expenditure when there is little data on meaningful local actions to engage community stakeholders. To encourage the expansion of local climate change engagement in cities, venues for sharing best practices have been set up to spur innovation. The carbonn Cities Climate Registry (cCCR) is an example of a global platform to report commitments, emissions levels, mitigation, and adaptation actions in order to ensure transparency, accountability, and comparability of results.[7] The Cities Alliance (including United Nations Environment Programme, the World Bank, and United Nations-Habitat) has also organized an online platform entitled 'Knowledge Centre on Cities and Climate Change (K4C).' K4C helps to track the progress of cities on addressing climate change, by serving as a platform for sharing experiences and best practices, as well as facilitating exchange of innovative initiatives. The cCCR and K4C have potential to highlight community level initiatives and expand data reporting and analysis to help them gain momentum by raising the profile of local city activities and demonstrating measurable progress.

Climate change stands as one of the most significant long-term threats to global infrastructure, impacting the natural environment, the built environment, economy, food security, and human health. In November 2015, international officials are expected to gather in Paris at the 21st Conference of the Parties to the UNFCCC with the goal of reaching a binding climate change agreement. Activities that focus on tying community-level activity in cities to international network activity will help strengthen the political will needed to provide a solid basis for this updated agreement and ensure funding. Providing an international voice to local city community work will provide a complex issue with the human story needed for the public to care more about it.❖

[6] C40Cities, Climate Leadership Group, http://www.c40cities.org/, accessed May 19, 2014.
[7] carbonn Cities Climate Registry, http://citiesclimateregistry.org, accessed May 19, 2014. The 'carbonn Cities Climate Registry' (cCCCR) began as part of the Mexico City Pact of 2010 at the World Mayors Summit on Climate.

The Center for Infrastructure Protection and Homeland Security (CIP/HS) works in conjunction with James Madison University and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The Center is funded by a grant from the National Institute of Standards and Technology (NIST).

If you would like to be added to the distribution list for *The CIP Report*, please click on this link:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1