INNOVATION IN THE "AGE OF ACCELERATIONS": GLOBAL RESILIENCE AND CYBER KNOWLEDGE NETWORKING

26-27 APRIL 2018

A Symposium and Workshop

Held by George Mason University, the Global Challenges Forum Foundation and the PfP Consortium Emerging Security Challenges Working Group in partnership with NATO Allied Command for Transformation,
and the United Nations Institute for Training and Research

CONFERENCE REPORT

George Mason University Science and Technology Campus
Manassas, Virginia

Background

Purpose

The *Partnership for Peace Consortium's Emerging Security Challenges Working Group*, the *Global Challenges Forum Foundation*, the *NATO Allied Command for Transformation* (NATO ACT), and the *United Nations Institute for Training and Research* (UNITAR) organized the second GKN conference. GNK II was hosted by George Mason University and took place on 26-27 April 2018 at the Science and Technology Campus in Manassas, Virginia.

This event built on a series of previous workshops and strategic dialogues in the United States, Europe and the Middle East that identified key challenges and pointed toward collectively owned opportunities. They began with the establishment of the "Global Resilience Readiness Initiative" at the launch of GKN in Geneva, Switzerland in September 2015. This was the 2nd GKN Symposium and was dedicated to the exploration of enhancing global resilience in the "Age of Accelerations." The sessions focused on ways that innovation, especially in cyberspace, can help future leaders, their organizations, and institutions address global security challenges in a complex world, by making knowledge actionable.

Day One was a Symposium with distinguished speakers and expert panels that created a framework for tangible progress on emerging security challenges and interconnected global problems.

- The *"Emerging Challenges"* Symposium commenced with the **Opening Keynote** on Cascading Risks by Dr. Stephen Flynn, who outlined that a strategic consequence of our increasingly hyper-connected world has been to elevate the risk of wide-ranging cascading failures from what once were largely localized disruptions
- The Symposium agenda on Day One set the stage for the **Featured Keynote** by Thomas Friedman on building resilience through ***"Innovation in the Age of Accelerations."***

Day Two was a design-thinking workshop, for invited attendees only. Actionable recommendations were developed by teams of invited experts building on the guidance of Pulitzer Prize Winner and keynote speaker Thomas Friedman.

Disruptions Will Happen

Dr. Ángel Cabrera, President, George Mason University, set the tone in his opening remarks to the second Global Knowledge Networking (GKN II) conference: Innovation in the "Age of Accelerations". He advised to "***Accept that disruption will happen and construct systems to deal well with the situation***". Innovation can help future leaders, their organizations, and institutions to meet global security challenges in a complex world, especially in cyberspace, as the goal is to make knowledge actionable.

Pulitzer Prize Winner and keynote speaker Thomas Friedman delivered his keynote speech, guiding the following group discussions of the invited experts:

> "Radical, rapid technology shift is leaving many people profoundly dislocated. Unless society finds new ways to respond to this dislocation, the sense of malaise and anger is likely to get worse, not least because technological change is speeding up, not slowing down. The upheaval today is far more dramatic than earlier phases. That is partly because of accelerating technological change, or the impact of "Moore's Law". But it is also because market forces are linking the world more powerfully than ever, occurring alongside three dangerous climate changes - one digital, one ecological, and one geo-economical. We have no choice but to learn to adapt to this new pace of change!"

GNK II built on a series of previous workshops and strategic dialogues in the United States, Europe and the Middle East leading to the establishment of the "*Global Resilience Readiness Initiative*" at the launch of Global Knowledge Networking in Geneva, Switzerland in September 2015. "*Age of Accelerations*", as the 2nd GKN Symposium has been dedicated to the exploration of enhancing local, regional and global resilience.

Pulitzer Prize Winner and Keynote Speaker Thomas Friedman's* "Mother Nature Model of Resilience"

Three climate changes

In his keynote address, Thomas Friedman spoke of three "climate changes" our world is currently going through:

1) The climate itself;
2) Globalization;
3) Technology.

In the midst of these 3 climate changes the old models of political parties have been broken: models like "left vs. right" date from the time of the French Revolution are not valid anymore. Even more recent models like "capital vs. labor", "deficit spending vs. fiscal responsibility", or "nationalist vs. internationalist" have broken down.

In this new reality, businesses need to:

- Optimize
- Analyze
- Prophecy
- Customize
- Socialize
- Digitize/automate

Mother Nature's Resilience

Mr. Friedman introduced a "Mother Nature" model of resilience. He argued that Mother Nature is both propulsive and resilient, she is:

- *Adaptive*	it's not the strongest or smartest who survive, but the most adaptive
- *Entrepreneurial*	filling every niche with some kind of organism tailored to it, encouraging constant innovation
- *Pluralist*	the most diverse ecosystems are the most resilient
- Sustainable	everything is food. Efficient uses of resources over the long term are valued.
- *Circular*	attuned to the direction and pace of change. Early and frequent detection of changes is a competitive advantage.
- *Hybrid and heterodox*	trying anything, non-dogmatic, supporting what works.
- *Allowing bankruptcy*	nature kills her failures and uses them to nourish successes.

Mother nature is not centrist. She uses some things that are very conservative and some that are very innovative: there is not a preference for the "middle." On the "left", she would support free health care and life-long free post-secondary education. On the "right", she would eliminate corporate taxes and encourage entrepreneurship. She would pay for a safety net with taxes on carbon, sugar, bullets, etc.

**Thomas Friedman is a regular contributor of columns on foreign affairs and columns for 'The New York Times'. He is known for supporting a negotiation armistice between Israel and the Palestinians, renewal of the Arab world, ecological matters and globalization. He is the author of six bestselling books that address various aspects of international politics and major shifts in the future world order, from a centrist, liberal perspective on American political spectrum. Apart from his career as a writer and columnist, he also served as a visiting lecturer at Harvard University.*

Thomas Friedman is the proud recipient of numerous awards and a 3-times Pulitzer Prize winner.

Emerging Security Challenges

The new world is violent and chaotic. As connections have become more interdependent, local shocks cascade and amplify. When anxiety goes up, people want to disengage. Consequently, resilience today must deal with uncertainty and ambiguity.

"The threat landscape today is very different from the strategic landscape in 2010."

Terrorism has become an enduring challenge, enhanced by returning fighters. New tech – robotics, hypersonic, artificial intelligence, predictive analysis, data-to-decisions, 3D printing, nano, DNA editing, robotics, VR, AR, AI, IoT, quantum computing, brain-computer interface, bio-hacking, electronic warfare, computer network operations, signal intelligence, psyops, deception etc. – enforces the need for permanent adaptation and modernization. China has become a significant global actor. An assertive Russia owns remarkable hybrid warfare skills to include military capabilities in all domains, particularly noticeable in A2/AD and Electronic Warfare. Noteworthy, regional powers such as Iran, have been developing capabilities of concern, such as Cyber, NBC, BMD, A2AD, to include hybrid warfare.

There are a diverse and growing array of threats to traditional and cyber infrastructure. A consequence of a digitally aware and engaged citizenry is increased understanding of threats. In addition, bad actors have more access to information to create disruptions than at any point in human history. The overwhelming amount of potential threat information creates apathy in a digitally engaged citizenry. Even with access to information, threat calculus is clouded by denial, lack of trust (in media and government), and paranoia. Individuals disengage because of anxiety and information overload. Digitally connected citizens are ignoring threats in a time where they have more access to information about them than at any time in human history.

The military is equally nonresponsive to evolving threats. Militaries are focused on traditional military to military combat scenarios. They seek tradition definable threats such as bad state actors. When their common institution enemy allies begin to turn in on themselves. Militaries are ill prepared to deal with small threats traditional and cyber infrastructure that could develop into a major crisis.

"Roughly 70% of resilience is cyber related."

Against this background, cyber has evolved as Tier 1 threat. Roughly 70% of resilience is cyber related. The understanding of the cyber domain needs to move from mission assurance to operational capabilities, while the big shortage is in particular on areas bridging domains. Consequently, the Cyber Defense Pledge needs to

- Address critical infrastructure
- Prioritize resources
- Acknowledge cyber space as operational space
- Reflect greater recognition that the battlefield has battlespace become increasingly digital
- Rely on offensive capabilities

Against this background **agility and speed of decision-making and action** have become key requirements that now need to be spelled out**.** What kind of pre-approval can be given, especially in missile defense? What about deterrence in world of complex hybrid threats? How manage risks within connections?

Risks can only be eliminated by investing enough muscle, intellect, money. While in security focus is top down and restrictive, in resilience it needs to be bottom-up and inclusive. A strategic consequence of the increasingly hyper-connected world has been to elevate the risk of wide-ranging cascading failures from what once were largely localized disruptions. This, in turn, is fueling a general sense of public anxiety. The perceived risks associated with globalization are increasingly being viewed as greater than the benefits. This growing sense of public anxiety is being tapped and fueled by national leaders who engage in the politics of fear, resulting in eroding support for open borders, free trade, and democratic institutions. The rush to embrace recent developments such as "Internet of Things" and "Artificial Intelligence" without adequate consideration of the relevant security implications and their disruptive potential appears to accelerate this trend.

Opening Keynote Speaker Dr. Stephen Flynn* on "Cascading Risks"

Hyper-connectivity and public anxiety

Today, we are living in a hyperconnected world. We choose to connect because we believe there is a benefit from it. We believe the risk of not connecting outpaces the risk of doing so. A local shock today can cascade and amplify in unforseen ways: we are not good at forseeing it.

A strategic consequence of our increasingly hyper-connected world has been to elevate the risk of wide-ranging cascading failures from what once were largely localized disruptions. This, in turn, is fueling a general sense of public anxiety where the perceived risks associated with globalization are increasingly being viewed as greater than the benefits.

This growing sense of public anxiety is being tapped and fueled by national leaders who engage in the politics of fear, resulting in eroding support for open borders, free trade, and democratic institutions. Left unchecked, the headlong rush to embrace IoT and AI without adequate consideration of some of the security implications and their disruptive potential, risks accelerating this trend.

Adversaries know this and they are looking for the very vulnarabilities that can lead to the biggest cascading errors. We need to understand that we cannot be 100 % secure. Security is not a zero sum game.

Moving from a threat-centered approach to a resilience-focused approach.

The way forward requires embracing measures that advance individual, community, and system/network resilience that collectively provide a sense of confidence that risks can be managed well enough that we can continue to live and prosper in an open and connected world.

threat = intent x capability

After 9/11 all resources were focused on trying to eliminate the threat and not on reducing vulnarabilities. Reducing our vulnerability means that the adversary needs more capability, in turn reduce consequences.

risk = threat x vulnerability x consequences

Investment in resilience can serve as deterrence AND make asymmetric threats less terrifying. To build societal resilience, we need to oversome five critical barriers:

- Risk illiteracy and pervasive lack of understanding of interdependent systems.
- Inadequate designs
- Pervasive economic disincentives for investing in resilience
- Inadequate governance frameworks and policy guidance to foster resilience
- Lack of adequate training and education to support the development and implementation of tools, applications, processes and policies for advancing resilience

* *Dr. Stephen Flynn is the founding director of the Global Resilience Institute at Northeastern University where he leads a major university-wide research initiative to inform and advance societal resilience in the face of growing human-made and naturally-occurring turbulence. At Northeastern, he is also professor of political science with faculty affiliations in the*
Department of Civil and Environmental Engineering and the School of Public
Policy and Urban Affairs, and co-director, George J. Kostas Research Institute for Homeland Security.

Dr. Flynn is recognized as one of the world's leading experts on critical infrastructure and supply chain security and resilience.

A Resilience-Centered Approach

The way forward requires embracing measures on the strategic, operational and local level - measures that advance individual, community, and system/network resilience that collectively provide a sense of confidence that risks can be managed well enough that societies can continue to live and prosper in an open and connected world.

Resilience is the catchword addressing this complex challenge. Yet, the current state of resilience efforts is overly reactive in scope and scale as the current understanding of resilience is proving inadequate and leads to ineffective efforts to implement policy. Resilience can no longer translate into waiting for damage to be done, paying for it, and socializing the cost. Resilience of the future is about inventing the future. To achieve this, Tom Friedman's group of "learning systems, training systems, management systems, social safety nets and government regulations" must be tuned to fast-changing conditions.

"Resilience of the future is about inventing the future."

Four major threats

Clearly, solutions need to address the four major threats that have been driving resilience requirements:

- Urbanization
- Aging infrastructure,
- Quality of live issue and
- Safety and security.

Governments don't own a lot of the critical infrastructure. With view to ensured services and business continuity private action can and should lead to public good. Massive migration to urban terrains, job loss, disruptive developments and natural disasters highlight: **RESILIENCE CAN'T BE DONE UNLESS IT'S BOTTOM UP AND INCLUSIVE.**

In the military seamless integration of domains below the level of conflict and higher operational tempo have become driving factors. As NATO and its member states move from mission assurance to risk management approach, it has to be assumed that systems may be degraded in crisis and conflict, particularly as NATO has an analog hangover. Clearly, there is a need for investing in new skills to bridge existing and further developing technical and strategic gaps. Recent developments show that NATO needs to walk away from the old view that it could eliminate risks. Obviously this doesn't work. Consequently, situational awareness, risk management need to feed a **Multi-Domain Battle Concept**.

"Recent developments show that NATO needs to walk away from the old view that it could eliminate risks."

Barriers to resilience

Building islands of resilience in a sea of fragility, violence and chaos may be a promising approach, as local shocks will likely have wide ranges. Building societal as military resilience requires overcoming critical barriers such as

- risk illiteracy and pervasive lack of understanding of interdependent systems
- inadequate designs
- Pervasive disincentives for investing in resilience
- inadequate governance frameworks and policy guidance to foster resilience
- economic disincentives
- lack of adequate training and education

to support the development and implementation of tools, applications, processes and policies for advancing resilience.

As managing risks is at the core of the resilience challenge this requires to move from a threat centric approach to a resilience-centric approach, to reduce vulnerability, reduce consequences and consequently reduce intent. To this end a couple of questions need to be addressed: What's

critical? What could affect us? What's valuable? What's vulnerable? What's our plan do deal with this? How to recover quickly?

To put resilience into practice we need to

- Adapt
- Prepare
- Mitigate
- Respond

in order to create effective processes and get practitioners assembled to do the job in a proactive resilience approach. In an info-fatigue environment resilience needs to be tough and about inventing the future you want.

Eliminating barriers through knowledge networks

Key to success will be knowledge sharing. This is a major challenge that requires steadfastness as a clearly defined objective. “Stove piped” and “siloed” information impedes the process of developing resilience. All involved stakeholders and groups must start the process of eliminating barriers block information sharing that should include

- A common set of facts
- Information that is verified and validated
- Only useful information and knowledge
- A cohesive and comprehensive community
- A shared contextual appreciation
- Crisis management processes, techniques, and models

The development of a network that responsibly shares quality information will incentivize participation - quality information that is delivered on a consistent basis thus establishing trust across nodes. Communication will be shared if quality information is flowing across the network. Access to a network with quality information will serve as an incentive to encourage knowledge sharing.

“Stove-piped and siloed information impedes the process of developing resilience.”

To create better communication networks is to increase collaboration. This has technical aspects – as proven with the famous Afghan Mission Network. But also partnerships are of essence. These must span the globe and be part of a new articulated paradigm based on sharing. Once organizations agree to form informal and/or formal relationships, shared agendas should be developed thus creating a culture that encourages the act of sharing knowledge online.

Towards Resilience Readiness – Educating, Training, Networking

Enhancing resilience has become an urgent and a strategic task. There is a danger of societal disruption with view to unemployment, widening gap between poor and rich, and not at least left behind citizens. To seize disruptive technology for inclusive development it requires informed, future-oriented decision making on all levels of International Organizations, nations, cities, private sector, etc. Consequently we need to educate the principles of self-org, knowledge-sharing, adaptive systems.

“Education needs to promote the ability to continuously learn and adapt, thus preparing individuals to acquire and shed rapidly changing skills requirements.”

Obviously, the current model of education - built on the process of codifying knowledge, inventorying skills, and transferring existing understanding to create a deployable workforce - is coming to an end. As machine intelligence advances, humans will offload work to machines, and then adapt, re-skill, and redeploy to new, uniquely human work. That process of adaptation requires a foundation in learning agility and a mindset that prepares them for change. Education needs to promote the ability to continuously learn and adapt, thus preparing individuals to acquire and shed rapidly changing skills requirements.

The drivers of disruptive change

Disruptive change will be driven by three interlocking factors that will likely transform our professional framework:

- ***Atomization:*** Secure and benefits-rich jobs will be the exception. Rather, work and professional tasks will be broken into fragments that can be done anywhere in the world by the best suited, available or lowest cost providers. Examples of atomized work are already available today at every skill level from driving a, providing digital skills to conducting business analysis, evaluation or strategy.[1]
- ***Automation:*** Much work will be done entirely by machines. While there are plenty of examples with factory robots that replace human labor, it appeared to many that knowledge labor would be immune to automation. The opposite is true. From automated insights at Associated Press to customer service chat bots as well as virtual assistants - we are just beginning to feel the impacts of automation regarding physical and knowledge-based tasks.
- ***Augmentation:*** New partnerships develop between machine intelligence and human workers to more efficiently and accurately perform jobs. Students, clinicians and surgeons already take advantage of these capabilities. Soon augmentation will touch virtually every aspect of work.

Within a new culture of globalization, we cannot teach for the future with the ways of the past, as we are in danger of alienating millions of young people who don't see education as the route to a good job. Innovation needs to get hammered out beginning in kindergarten and continuing in schools and professional education and training. With view to cyber, we need training through a Multi-domain E*ffects-Based* Lens. Consequently, the future of work and learning will focus on scalable learning with agility.

Educating for the future

Agile mindset need to focus on cultivating adaptive learners who can leverage the uniquely human skills of **Empathy** (to find new needs), **Divergent thinking** (to find and frame problems not yet known), **Entrepreneurial outlook** (to turn discovered needs into sustainable value), and **Social and emotional intelligence** (to adapt and thrive in a world that is increasingly volatile, uncertain, complex, and ambiguous).

"The lesson from Fukushima is: build capacity at the local level."

The right mindset provides safe harbor in a sea of disruption. It enables graduates to make sense of shifting context and to recast their story so that they can march back to relevance. It enables decision makers to identify the valid context for their decisions. This continuous reinvention will dominate the future of security and prosperity, the future of our life. And developing empathy for yourself and the grit to manage your internal critic will separate those who are successful in the future with those who struggle.

Consequently, we need to take resilience, i.e. cyber resilience, to the next level. We need a cyber revolution at the local level. Clearly resilience needs to be provided on the national and international level. But this is not enough. There also needs to be focus on the local level, as it is mayors, private sector companies, etc. who are facing the risks, not knowing what to do. The lesson from Fukushima is: **build capacity at the local level.**

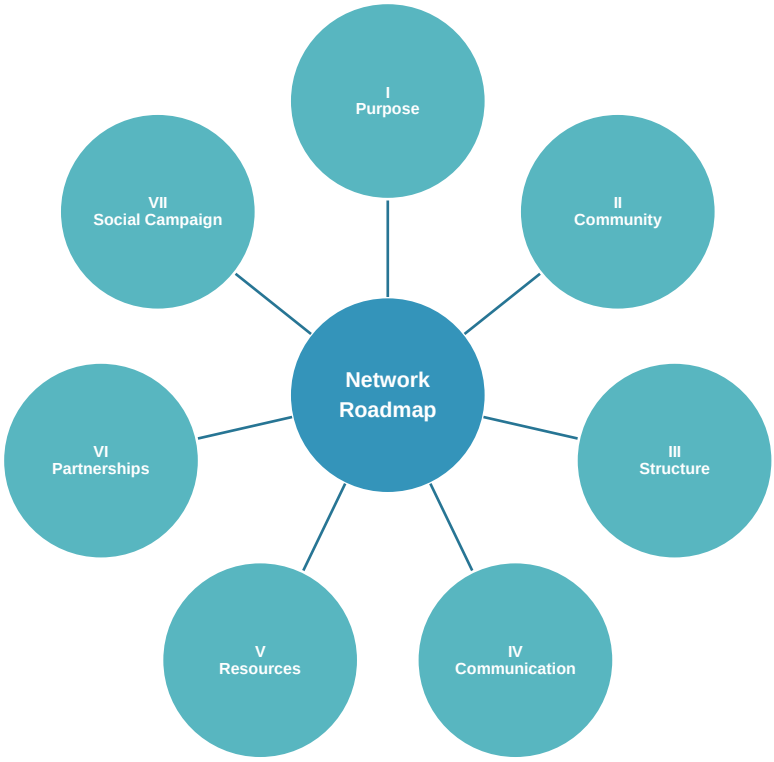
Workshop Recommendations

Forty-five professionals, with diverse backgrounds, participated in a condensed design workshop the second day of the 2nd GKN Symposium organized by the PfP-C Emerging Security Challenges Working Group. The group broke into five teams to provide recommendations on the following **Opportunity Statement:**

[1] Lawrence F. Katz (Harvard University) and Alan B. Krueger (Princeton University and NBER)

How might we leverage the expertise, networks and energies of the Cyber Knowledge Networking Workshop into a sustainable community able to grow organically in support of 21st Global Knowledge Networking.

The design technique allowed the group to analyze the impact and the feasibility of each part. The seven parts, listed from the most impactful to the least impactful, include: community, purpose, resources, partnership, communication, structure of organization, and social campaign. Listed by most feasible to the least feasible, include: community, communication, structure of organization, social campaign, purpose, resources, and partnership. The group recognized a sense of belonging, as the primary motivator driving the workshop was the desire to create a sustainable community. The group selected purpose as the first step in a critical path toward the formation of a sustainable community.



Below is a synthesis of their findings and recommendations. It emerges in a seven-part roadmap to support the steps toward the creation of a sustainable community of practice for global resilience and could be the basis for future working group meetings, including the 3rd GKN Symposium planned for Abu Dhabi in 2019.

I. Purpose

The synthesis includes the following ideas as possibilities for the recommended purpose(s):

- provide the required organizational structure;
- foster the proliferation of innovative thinking;
- empower a community of innovation and design practice;
- promote the sharing of best practices;
- create a central hub for all things innovation;
- capacitate a center of a design culture for sharing cyber knowledge in support of global resilience;
- nurture the growth of an international community of study;
- enable the creation of human centered collaborative teams;
- facilitate the expansion of greater military capability;
- preserve the application of military reflexive practice;
- advance the integration of design thinking in the curriculum of professional military education.

The teams recognized the selection of a purpose or set of purposes as one of the more challenging tasks. However, after the selection of an established purpose or set of purposes, the answers to the questions of who, what, when, and how become easier. Those options are listed below for each of the remaining six areas.

II. Community

The synthesis includes the following ideas as possibilities for the key attributes of our community:

- strong leadership;
- reservoir of subject matter experts;
- strong outreach with community to community exchanges of information and expertise;
- rewarding network opportunities;
- exciting work and topics of interest;
- receptive audience;
- healthy mentoring;
- grassroots inclusion.

III. Structure

The synthesis includes the following ideas as possibilities for the structure of an organization:

- formulation of a committee on organizational framework;
- creation of a charter and by-laws;
    - identify all critical positions with roles and responsibilities;
    - include a member's bill of rights and responsibilities;
    - ensure international scope;
    - allow for the possibility of multiple partners while ensuring independence;
- election of board of directors;
- election of key leaders and workers;
- development of a vision with steady state goals;

IV. Communication

The synthesis includes the following ideas as possibilities for the critical communication requirements:

- build and operate an open communication network;
- create a plan for a sustainable and active webpage;
- institute pathways for publication opportunities;
- construct forums to increase the strength of the community;
- develop a phone application to support community dialogue;

V. Resources

The synthesis includes the following ideas as possibilities for the critical resource requirements:

- leverage price sharing through annual membership dues and other fundraising activities;
- Include fees as part of participation in community gatherings;
- depend on volunteers to provide pro bono services;
- solicit corporate sponsors on an individual event by event basis;

VI. Partnerships

The synthesis includes the following ideas as possibilities for the recommended features of partnership agreements:

- create an order of merit list for the targets of resource extraction and consider the following as selection criteria:

    - place primacy on international, government, and defense organizations;
    - consider a permanent and exclusive partner of choice;
    - select partners based on assured access to resources;
    - seek grants and other sources of monetary academic support;
- established memorandum of agreements approved by a majority of membership;

VII. Social Campaign

The synthesis includes the following ideas as possibilities for the recommended aspects of a social campaign:

- identify opportunities;
- leverage internal organizational talent;
- maintain stimulating programming;
- market to lowest levels;

Suggested Framework and Next Steps

Consequently, it becomes important to develop the courage to invest and experiment. The GKN II symposium delivered two actionable outcomes that are presented below.

"The GKN II symposium delivered two actionable outcomes."

OUTCOME 1: Proposal for a Global Network of Resilience Readiness Centers

In the context of growing numbers of local, regional and global shocks and stresses, resilience deals with how to prepare, recover and learn & adapt before, during and after they materialize. At the heart of resilient systems lie knowledge, effective partnerships and future oriented decision-making. The Network of Resilience Readiness Centers (RRCs) could serve as an integrated global framework for common decision-making, opposed to ad hoc solutions that mostly cannot be tailored for each specific type of risk.

While facilitating systemic understanding and strong lateral connectivity, it provides for transparent and effective ways to tackle the issues at hand and helps to create a shared consciousness leading to sustained impact. As such it fosters general decision-making, observing not only the development of specific risks, but rather contributing to a comprehensive ability to identify and handle newly emerging risks as well.

Mission statement

Within the global network of regional RRCs, strong focus is laid on making use of existing networks and their concentrated synergies, as opposed to duplicating them. The RRCs form a technologically linked, global and virtual network that helps to foster communities of practice without duplicating present solutions but rather serving as an integrator of existing platforms and networks. Each RRC is envisioned to be a nimble hub, supplemented by being part of a composable organization that can be modified or reorganized based on the needs of the moment and that brings together selected partners of excellence.

As a hub for knowledge surrounding resilience, the RRCs have the following missions:

(1) Ad-hoc advice for acting leaders in a crisis;

(2) Education and training of today's leaders;

(3) Education of tomorrow's leaders.

Location

The respective locations for RRCs are selected carefully as to make use of already existing networks and of expertise and technical capacities. The RRCs added value stems from the trust and collaboration developing because of the synergy created between technologies, people, and ideas and enabling the cultivation of new partnerships better able to bring swift resolution to complex crises. Decentralized execution occurs as each region develops distinctive approaches. This approach will be first applied in the proposed RRC pilot project: The Gulf Resilience Readiness Center.

Global Challenges Situation Room

Making knowledge both available and actionable for political, societal and economic decision-makers is of key importance in a time of rising ambiguity, black swans and hybrid threats. **The Global Challenges Situation Room** is a unique strategic analysis instrument for the collaborative management of risks. It is the central entity in the Network of Networks of RRCs and is intended to assist national governments, business leaders, organizations in civil society, and private citizens directly in identifying, understanding and assessing global risks.

The Room's working logic can be compared to that of a particle collider. A permanent team operates and provides the infrastructure for a second, rotating team of domain experts who are working temporarily and event-driven on specific tasks. These tasks are to identify, asses and understand emerging challenges. Making use of the support and the advanced infrastructure provided by the Room and the surrounding Network of Networks of the RRCs, the domain experts are empowered to identify and assess risks that can then be shared convincingly with various stakeholders and decision-makers.

OUTCOME 2: The GCF-UNITAR Global Resilience Consortium

A) Partnership Agreement between GCF and UNITAR

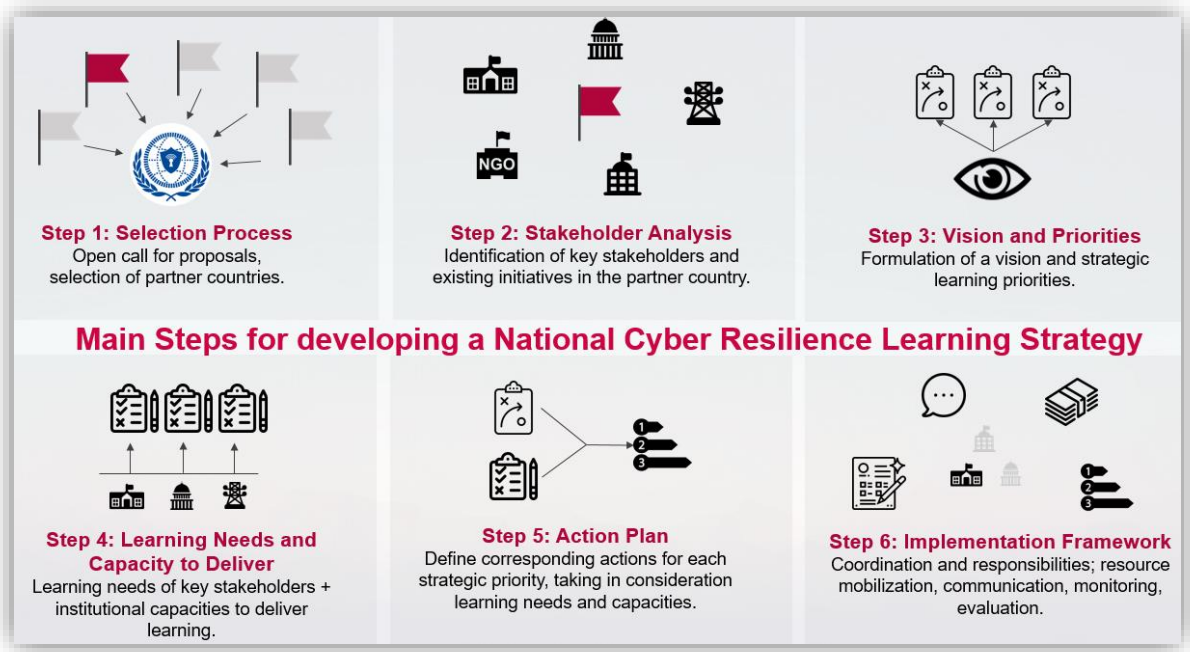
The United Nations Institute for Training and Research (UNITAR) and the Global Challenges Forum Foundation (GCF) signed a three-year Memorandum of Understanding (MoU) to provide a cooperative framework in form of a "*Global Resilience Consortium*" within which the Parties can develop and implement activities in support of the "Geneva Declaration" concerning the Global Resilience Readiness Initiative (Appendix 1). With the MoU, GCF and UNITAR also commit to develop and implement a joint capacity-building program in cybersecurity (see below) and to jointly pursue cooperation based on their respective mandates, mission, goals, needs, expertise, networks and work programs. Specifically, UNITAR will provide support to the GCF's fundraising activities by providing technical guidance to prepare funding proposals and GCF will facilitate UNITAR's access to technical partners for the development of training materials on cybersecurity.

The United Nations, in the past, has emphasized the crucial need for capacity building in the cyber realm. Recently, the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security reiterated the vital importance of capacity building to securing ICTs and their use. Consequently, the group recommends states to support "the development and use of e-learning, training and awareness-raising with respect to ICT security. Consequently, GCF and UNITAR are eager to cooperate with in this arena that is so important to achieving the 2030 Agenda, and to combining their expertise in the fields of cybersecurity and capacity-building, respectively.

B) Cyber Capacity Building on the Local Level - United Nations Cyber:Learn

As a first deliverable of the MoU mentioned above, representatives from the Global Challenges Forum Foundation and the United Nations Institute for Training and Research presented a joint project that was incepted at the GKN II planning workshop at the National Defense University in Washington DC

in 2017. The project consists of a United Nations Cyber Resilience Learning Platform (UN Cyber:Learn, www.uncyberlearn.org) for the local level.



UN Cyber:Learn aims to improve inter-institutional and cross-sectoral knowledge exchange and to promote a strategic approach to cyber resilience. It bundles available learning resources and knowledge on cyber resilience in one single place and supports both e-learning and face to face courses and workshops on cyber resilience and related topics. The platform builds upon UNITAR's extensive experience in developing online tools that aim at strengthening capacity building and at developing communities of practice and on GCF's strong network of senior experts in the cyber domain. UN Cyber:Learn has three planned outcomes:

1) Developing Capacity for Cyber Resilience at the Local Level

Capacity in the cyber domain is critical for progress in economic, political and social spheres and indispensable for building resilience. UN Cyber:Learn builds on targeted capacity building to leverage the benefits of education and training to enhance cyber resilience.

2) Networking Actors and Capabilities & Creating a Shared Knowledge Process

Resilience and knowledge go hand in hand. Without a common reference point, collaboration is rendered difficult and relevant knowledge created in one domain might go unnoticed in another. UN Cyber:Learn is designed to create and to cultivate a wide array of partnerships as an ecosystem for a shared knowledge process.

3) Promoting a Strategic Approach to Cyber Resilience

As technology increasingly permeates into every aspect of our lives, responses need to be sought on the highest levels: cyber resilience depends on strategic, long-term thinking. UN Cyber:Learn supports the development of strategies for cyber resilience in local governments and organizations.

UN Cyber:Learn provides support for developing and implementing National Cyber Resilience Learning Strategies. Such strategies identify actions to be taken in the short, medium and long-term to strengthen the human resource base to strategically increase cyber resilience. The main steps for developing such strategies are illustrated above. The activities are carried out in a country-driven process and the strategy will be linked to preexisting initiatives and rely on broad institutional participation, ensuring that ownership remains with the country and resilience is built bottom-up.

Appendix

THE GLOBAL CHALLENGES FORUM
"GENEVA DECLARATION"

PREAMBLE:

Meeting in Geneva, Switzerland, on 16 and 17 September 2015, against the background of an escalating refugee crisis in Europe, the Global Challenges Foundation and the United Nations Institute for Training and Research (UNITAR) co-hosted the Launch of the Global Knowledge Networking Initiative in collaboration with the U.S. Department of Defense (DoD) and the Middlebury Institute of International Studies at Monterey (MIIS).

In support, they invited a distinguished and diverse group of experts from around the world to guide the way ahead and convened its Inaugural Conference entitled, ***"Toward a Smart Century: Global Partnerships for Innovative Learning and Leader Development."*** Participants helped to shape a broad understanding of the continuing role that Global Knowledge Networking (GKN) should play in empowering future leaders, their organizations, and institutions to address global challenges through integrated approaches that make knowledge manageable and actionable.

The Inaugural Conference explored the means of promoting greater resilience to complex emergencies and shared global threats posed to the environment, human security (including health), maritime and cyber security, and energy security, as well as challenges posed by terrorism and hybrid warfare. A shared understanding emerged that humankind is moving quickly towards a knowledge-based Smart Society in which the networking and cross-fertilization of ideas through an innovative education and training development hub can foster smart collaboration. A dynamic approach to the discovery and co-development of new capabilities can help build trust and collaboration among many cities and nations, effectively empowering readiness through enhanced community resilience, connecting generations, and cultivating a wide array of new global partnerships.

The Inaugural Conference, therefore, decided to create this future, concluding that new pathways toward holistic, cross-discipline and divergent thinking--which can empower connectivity, information sharing and fusion through a comprehensive approach--must be pursued. Having achieved consensus that a smart security, global knowledge capability is needed, the Inaugural Conference established the ***Global Resilience Readiness Initiative***.

ESTABLISHMENT OF THE GLOBAL RESILIENCE READINESS INITIATIVE

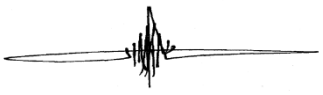
To foster imagination and discovery, produce enlightened experience, prevent conflict and promote sustainable development, the Inaugural Conference established the ***Global Resilience Readiness Initiative*** with the aims and goals to:

- Support community decision-making in partner nations and in international bodies through *"composable organizations,"* where people, ideas, processes and technology can be brought together as needed;
- Pursue "whole of stakeholders" approaches and enhanced information sharing in the area of disaster preparedness;
- Build new learning tools with partners to improve common understanding and shared procedures for rapid, decisive, resilient responses to complex emergencies;
- Contribute to significantly enhanced training and readiness capabilities for security and resilience through co-development of a global network of regional Resilience Readiness Centres;
- Evolve to meet new security challenges, and in particular adapt to the pace of change of information and communications technology (ICT) that underpins the development of the Smart Society.

The Inaugural Conference requested the Chairman of the Global Challenges Forum (GCF) Foundation to serve as Executive Director of the ***Global Resilience Readiness Initiative***, and to undertake consultation with global cities, nations, international bodies and other major institutions engaged in promoting innovative learning and leader development.

As an initiative of the Global Challenges Forum Foundation, all subsequent activities will be carried out in accordance with the applicable laws and regulations of the Canton of Geneva or other legal jurisdictions as may be appropriate. We will continue to reach out to the UN Institute for Training and Research, the US Department of Defense, the Middlebury Institute of International Studies at Monterey, and other Inaugural Conference collaborating organizations for guidance and support.

All Inaugural Conference Participants are invited to join in as Founding Members. This Declaration is made by the Undersigned on behalf of the Global Challenges Forum Foundation and the Global Knowledge Networking Inaugural Conference.



TALAL ABU GHAZALEH
Founder and Honorary Chairman

WALTER L. CHRISTMAN
Co-Founder and Chairman