Cyber Future Foundation

09/09/2016

Input to the Commission on Enhancing National Cybersecurity

Board of Directors, Cyber Future Foundation

Future of Cyber What are WE Aspiring and How do WE Achieve our Goals in Cyber in the Next Decade?

CFF Point of View on Future of Cyber

- Cyber Future – Why Digital Pivots on Cyber
- Cyber transcends Digital in creating value
- Areas of focus for Cyber at National and Global Level
- Focus on national cyber interest current and future state
- Additional macro cyber areas to consider
- CFF's role in building the future of cyber

Executive Letter to the Commission on Enhancing National Cybersecurity

The Honorable Chairman & Commissioners,
Commission on Enhancing National Cybersecurity

It is our honor and privilege to submit our response to the request for information regarding cybersecurity as a matter of national interest, and hope that it will add to the collective inputs towards formulating robust cybersecurity policies and practices at every level of the nation's digital economy.

At CFF we believe that as a human race we will continue to thrive not only our physical abode, which is earth, that we occupy, but it will exert itself to greater aspirations in the virtual domain, that is cyberspace. While our physical limitations may be a hindrance to our individual aspiration, human mind and its unfathomable psyche can achieve and attain feats that are limitless. When working in harmony with other creative beings, the human race with access to cyberspace, as defined by the time and talent of those engaged, can and will take the entire mankind to greater heights (or deeper abyss, depending on how the resources and faculties are used).

We believe every individual in this planet should have the opportunity to have access to the digital resources in the cyberspace and use it collaboratively for the greater good of mankind. And it is our prerogative as the leader of idea and innovation, to ensure safe and secure online access to the cyberspace.

We believe the best way to achieve these goals is to encourage initiatives by promoting greater access to the cyberspace; to promote collaboration among the commercial, government and academic sectors engaged in digital commerce and cyber infrastructure building; and to ensure participation by citizens of the world from diverse communities and all levels of society. In our experience, such collaborative and collective pursuit help build common ethos, achieve excellence (in their common goals), enable people to apply themselves to a greater good and use the digital and cyber assets for the nation and in general – to the betterment of mankind and society.

This is a condensed version of our point of view only addressing areas of focus from the commission, for updated and more comprehensive point of view with global and macro areas of focus, the honorable Commission and public are encouraged to visit www.cyberfuturefoundation.org periodically.

Yours Sincerely,
Val Mukherjee, CISSP, CRISC
Chairman, Cyber Future Foundation
www.cyberfuturefoundation.org

The Challenge facing us and what problem do we need to Solve for our Community and the Greater World … The Cyber-Digital Divide

Cyber threats and challenges are looming in today's Digital Age! Yes … Looming …

We cannot stop **complaining about Cyber** on the other hand cannot Stop **Fascinating about Digital**!

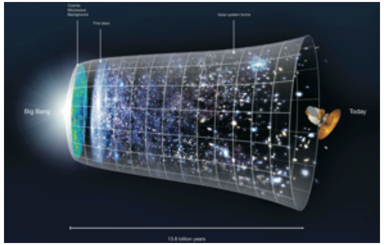
Digital cannot exist without the connectedness of **cyber**. Digital in Isolation makes Digitization of assets completely irrelevant.

Cyber	Digital

Two Sides of the same Coin – Yes … Even BitCoin!*

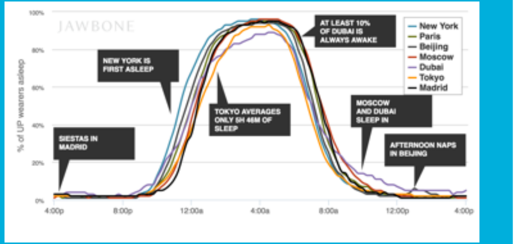
*IMAGE: FLICKR, ANTANA

How Awesome is Cyber! >> Future Forward Cyberspace … Consider ‘How we Got to Now*’ in a Decade … 2025!



From Infinitesimally Small Quantum Computing

To Infinitely Large String Theory



From Individual Personal Health Data

To Demographic Health Patterns and Information

From Smart Homes for families

To Smart Cities for Citizens

From Individual Regional Cyber Efforts

To an integrated Global Collaborative Platform

The identified Critical areas of Focus for Cyber, we see them as individually significant, and collectively paramount

Identified Areas of National Interest	Critical Infrastructure Cybersecurity	Cybersecurity Insurance	Cybersecurity Research & Development	Cybersecurity Workforce	Federal Governance
	Identity and Access Management	International Markets	Internet of Things	Public Awareness & Education	State & Local Government Cybersecurity
Some Additional Macro Areas of Interest	Cyber Peace	Cyber Resilience	Cyber Trusted Ecosystem	Cyber Crime & Terrorism	Cyber Warfare and Deterrence

These and many more additional nuances of cyber and the future digital economy needs to be considered and addressed while developing policies, frameworks, guidance for markets and overall directions for a digital economy of the future moving at the speed of cyber

Areas of Identified Cyber Issues Now and in Future

Critical Infrastructure Cybersecurity is fundamental to our lives as individuals and of paramount importance to national security

Critical Infrastructure Cybersecurity

- Needs immediate technology refresh
- Prioritized Risk Based Approach
- With an eye towards a connected future

Current State

- The current state of cyber critical infrastructure including such sectors as Energy, Water, Transportation, Financial Services and others have received some tactical support from the Government and private sector
- Most of these critical infrastructure components, especially power and utilities are based on age old technologies that have not been refreshed due to the nature of their inherent architecture
- Government sponsored Volunteer efforts and regulatory enforcement have picked up steam lately, but not adequately

Future State

- The future of critical infrastructure cybersecurity requires a concerted effort and substantial redesigning of digital components to ensure that they can keep up with the dynamic nature of a connected cyberspace
- Some areas such as financial sector is poised to go through a significant change and possible disruption due to emergence of new digital economic infrastructure, especially digital currency and block chain technology
- Sectors such as Power and Utilities need to rethink and reshape their cyber capabilities as they get integrated into the consumerization and connectedness

Cybersecurity insurance is meant to provide an option to mitigate losses from a multitude of cyber ‘casualties’ and incidents

Cybersecurity Insurance

- Needs Cyber Actuarial
- Risk Based Assessment
- Preventative Approach for Cyber

Current State

- Cyber insurance is evolving as a mainstream risk mitigation component for enterprises
- Cyber insurance is not a very mature space as of now and needs a lot of statistical and actuarial data to support the determination of coverage & claims
- Cyber insurance as an industry in itself is learning through course corrections, however many major players are present to provide significant direction
- Still a standalone offering amongst other general areas of liability and casualty insurance
- Awareness and education from focus groups is helping steady advance in this domain

Future State

- A strong Cyberinsurance industry will promote the adoption of mature cyber practices and cyber hygiene leading to reduced risk of cyber casualties
- Cyber insurance providers will add on incentives for the mature practices
- Cyber insurance will develop cyber actuarial which will be driven by the type of incident and available recourse
- Cyber insurance will also need to have support from policies that provide safeguards around data protection and privacy, while allowing for cyber intelligence sharing
- A strong Risk Management framework which is akin to financial/business risk will drive the adoption of cyber insurance as we look forward to the future

For Cybersecurity Research and Development entrepreneurship and innovation is today's mainstay, future needs to be more thorough

Cybersecurity Research & Development

- Significant investment is required
- Innovation supported by Thorough Research
- More public-private-academic collaboration

Current State

- Cyber Research & Development is an up and coming topic and not yet the mainstay of innovation
- Innovation is currently fueled by an entrepreneurial spirit of addressing specific problems with widgets, and not comprehensive, fact/research based efforts
- There is a distinct gap in thorough academic research supported by diligent study of facts and figures
- Larger organizations are adopting some R&D initiatives, but the budget, effort and attention is usually directed towards the current operational needs – firefighting mode is a huge distraction for sustained innovation

Future State

- A concerted initiative, both in academia and industry over cybersecurity research and development needs to be established
- Academia and industry should collaborate in R&D efforts which would provide the academic incentive in making cybersecurity a mainstream area of research
- Academic research should be supported by industry orientation both in terms of hands of industry experience as well as the practical application of developed product to enterprise scale
- Students and Researchers should be incentivized to provide focused attention to cyber challenges not only in technology but across the board including but not limited to cyber economy, cyber governance, cyber policy, even cyber doctrines for military usage

With demand far outpacing supply, it is essential that we invest at every level in developing the cyberworkforce of the future

Cybersecurity Workforce

Cyber specialists need to be well rounded

Not Just technology but business SMEs needed

Need both academic and vocational curriculum

Current State

- Every sector of national economy is being challenged by cyber issues, and there is not enough people to serve the needs
- The academic output supporting cyber requirements for the job market is next to negligible if not nothing
- Cyberworkforce is too IT focused right now, and needs to be more thoroughly groomed with knowledge of business and risk
- Cyber also needs super specialized technologists who are well versed: trained and certified
- Areas requiring financial skills, risk management or security clearance in federal & critical infrastructure protection roles are even harder to fill

Future State

- Cyber initiatives for workforce development should be developed with public private academic collaboration
- Government needs to issue fact based guidance providing macro level economic requirement and support academic pursuits for cyber education
- Government initiatives should be supported by business to accelerate the time to value and productivity through apprenticeships
- Cyber curriculum should be included in the basic STEM/STEAM programs with balanced and well rounded focus on the needs of a connected cyber future
- Structured academic cyber curriculum needs to be supported by vocational studies supported by private industry which provides direct and timely supply of cyber workforce to the industry

Federal Governance needs to consider cyber as a strategic as well as operational component, and also needs to adjust to the dynamics

Federal Governance

Cyber resiliency is of great importance

Cyber maturity higher than ever before

Cyber governance need to be at speed of cyber

Current State

- Government infrastructure is equally if not more vulnerable, as demonstrated by series of breaches and disclosures
- Federal government has a steep slope to climb in terms of infrastructure updates
- There is a need to balance citizen's fundamental rights, privacy and security as i relates to the state (federal security)
- Cyber governance currently is quite archaic and time consuming processes needs to be adjusted to evolve quickly to address current needs
- There are initiatives by the federal government to quickly identify innovative solution and onboard them to federal platforms, this process needs to enter mainstream federal procurement process

Future State

- Federal Government will be expected keep up with the pace of digital disruption, both economy as well as societal changes, this needs to be supported by a strong cyber governance process
- Cyber governance has to have steady executive and legislative support in terms of policies and operational execution
- Governance process needs to include identification of digital trends, procurement of capabilities necessary, operationalization of adequate measures, including technologies, and refresh at a rate commensurate with the changes in a dynamic cyber world
- Technological innovation and adoption should be a part of the governance process, supported by a risk based decision making process
- Cybersecurity oversight and accountability must be ingrained into the leadership at every level

Identity – both of human and devices is key towards security and accountability of access, needs to be established and manifested

Identity and Access Management

Identity is the new cyber perimeter

Both device as well as human identity counts

Strong governance of identity & access is a must

Current State

- Identity has been established as the new perimeter of the corporate as well as consumer domains are struggling with protecting identity data
- Governance around corporate identity has many challenges – both operational processes and technological
- There is a need for a fundamental refresh in identity protection mechanisms – such as moving away from single factor knowledge based authentication mechanisms
- There is also an increase in the scale and variety of consumer identity which needs to be addressed in ways that are commensurate with the needs of the future consumer and individual

Future State

- Identities of human, devices and autonomous things that are connected to the cyberspace needs to be addressed in their respective context
- Safe cyber hygiene needs to be promoted across consumers and organizational end users as the boundaries between the two disappear
- Identity management should be supported by activity and context, through analytical intelligence support
- The concept of trusted identities need to be developed and supported by technological innovation to ensure they ease of use is supported by definitive security controls and measures
- Identities should be monitored for activities, but with due care for privacy concerns
- Identity management should embrace at least a multi factor approach and supported by some form of digital certificate and physical association

Cyberspace so far has no boundaries and is expected to remain so leading to unfettered access into the international markets

International Markets

- Cyber supply chain is as critical as physical
- International data laws and regulations are essential
- Economic & societal benefits are immense

Current State

- The current state of international market manifests itself in both flow of goods and knowledge, and it is supported by tremendous economic and societal/cultural in and outflows
- The current economy led by US global conglomerates and business houses dominate International markets and cyberspace provides unfettered access
- Most of the cyber space being open and boundary-less provides for free flow of knowledge
- However this also exposes the US businesses to the threats looming in the cyberspace – this pain is accentuated by cyber data breach and espionage activities, including theft of intellectual property from US businesses

Future State

- Chances are that the cyberspace will remain open and boundariless are high in the next decade, which will lead to continued increase in cross border economic activity through cyber
- Access to international markets will provide unlimited opportunities, but definitely potential for many challenges of goods and services that are not welcome
- Regulating the cyberspace to provide safe and secure access to international markets will be necessary to support the digital economy of the future

Internet of Things is at its infancy and already generating more data than we have ever done in the history of mankind

Internet of Things

Incredible amount of devices to be connected

Incredible amount of data already generated

Needs new architectures and paradigms of scale

Current State

- IoT evolution has been very rapid with an incredible amount of devices already connected to the ecosystem, generating an incredible amount of data
- This is hardly addressed by the current standards and frames of reference that the enterprise and consumer cyberspace is used to and able to manage
- IoT disrupts the current model of cyber by establishing a parallel device network shadowing the human connected network and the legacy controls are not applicable there
- IoT also provides an incredible opportunity aid the digital commerce

Future State

- IoT and the OT will continue to include a multitude of devices, which will result in device device as well as human device interaction, continuing to generate an incredible amount of data
- The data generated has to be resolved for various data sensitivities, regulations and privacy mandates, this is an area which IoT is extremely challenged at this point
- Future of IoT will also need the devices to be secure by design, leading to an overall secure IoT
- We except the agility and flexibility of cloud services both at infrastructure and software powering growth
- IoT will form an ecosystem as well as data platform to fuel the intelligence and information in cyberspace
- As maturity in IoT grows the vulnerabilities will reduce but initially it will be plagued with the same set of problems we have in the internet

Public awareness and education is critical, however strong technical controls are – human element is what serves as the weakest link

Current State

- Very little knowledge currently exists in the public realm
- Consumers are usually left to their own device in addressing cyber challenges
- Cyber education is fundamental but not addressed in the public education medium
- Cyber is seen as an evil and the bias leads to a negative attitude towards it overall

Future State

- Cyber awareness and education is going to be key to safe journey into and through to the cyber economy of the future
- General awareness aided by focused public campaigns of safe cyber practices will ensure general public is not led to dangers that can be avoided
- Enhanced safety for children and young adults for countering cyber exploitation and overexposure needs to be built in
- Both academic and public campaigns need to be supported by public-private partnership

State and Local Government will play an inevitably significant part in the cyberspace through public-private and individual interaction

State & Local Government Cybersecurity

- Connected and Accessible Government
- eGovernment enabled by cyber presence
- Ensuring local and state law enforcement

Current State

- State and local governments have a number of digital initiatives which seem to be operating on older infrastructure as well as architectural paradigms not safe for a connected cyber economy
- Safety and privacy of citizens is usually a state issue and needs to be addressed along with providing access to government infrastructure and services

Future State

- State and local governments will be more connected than ever before
- Government services will be made available more and more through the cyber/digital medium
- State and local governments could be custodians of digital identities due to capabilities for positive physical verification
- Initiatives such as connected digital cities will provide significant impetus to the cyber economy of the future

How CFF is Addressing the Cyber Needs of Future

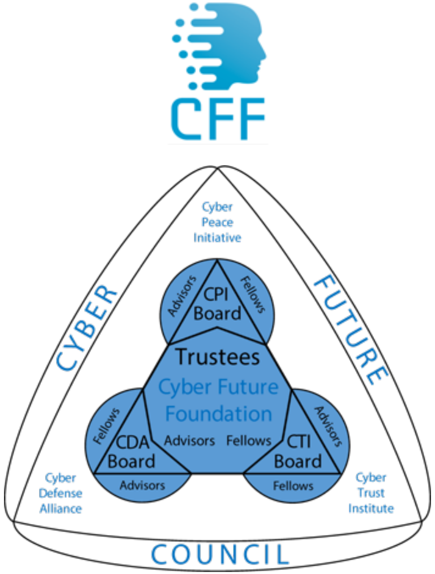
To Build a lasting Monument, you have to build an everlasting Foundation … Building Global Trusted Cyberspace, a step at a time

2016	2017	2018	2019	2020
Build Cyber Global Leadership Platform	Build Cyber Global Constituency Platform	Build Cyber Global Community Platform	Build Cyber Global Collaboration Platform	 Global Trusted Cyber Future Platform
•Build core leadership Team and engagement platform leading to global action	•The Core Leadership Group will take upon developing their respective constituency groups within CDA, CPI & CTI	•The Constituencies will address the needs of their respective communities and develop a global community of trusted cyber entities	•The communities will integrate their work products, action plans, outcomes into a global collaboration platform of trusted cyber entities at an individual as well as machine level	•The Cyber Global Collaboration platform will be dedicated to global action for leveraging across commercial, public, and community sectors towards trusted cyber commerce, communication, and collaboration

Finding Order from Chaos, and Structure from the Unstructured … And the Ability to Address Change at the Speed of Cyber

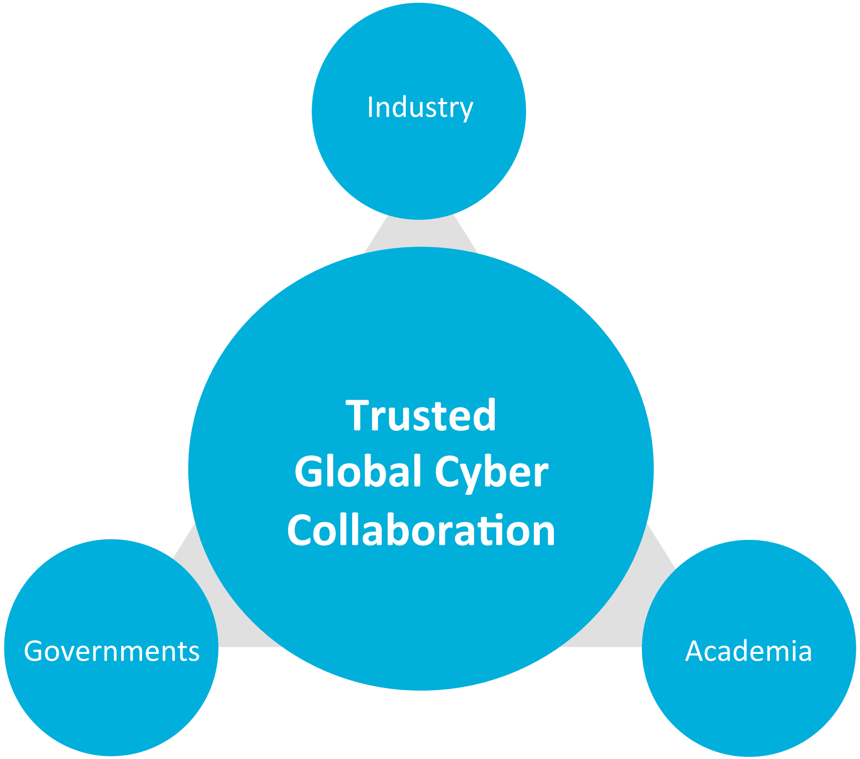
ISSA
Information Systems Security Association
ISACA®
Trust in, and value from, information systems
CSA cloud security alliance®
NIST
National Institute of Standards and Technology
U.S. Department of Commerce
SANS
(ISC)²®
SINET
Security Innovation Network

From a Global Collection of Cyber Efforts from Various Best in Class Organizations



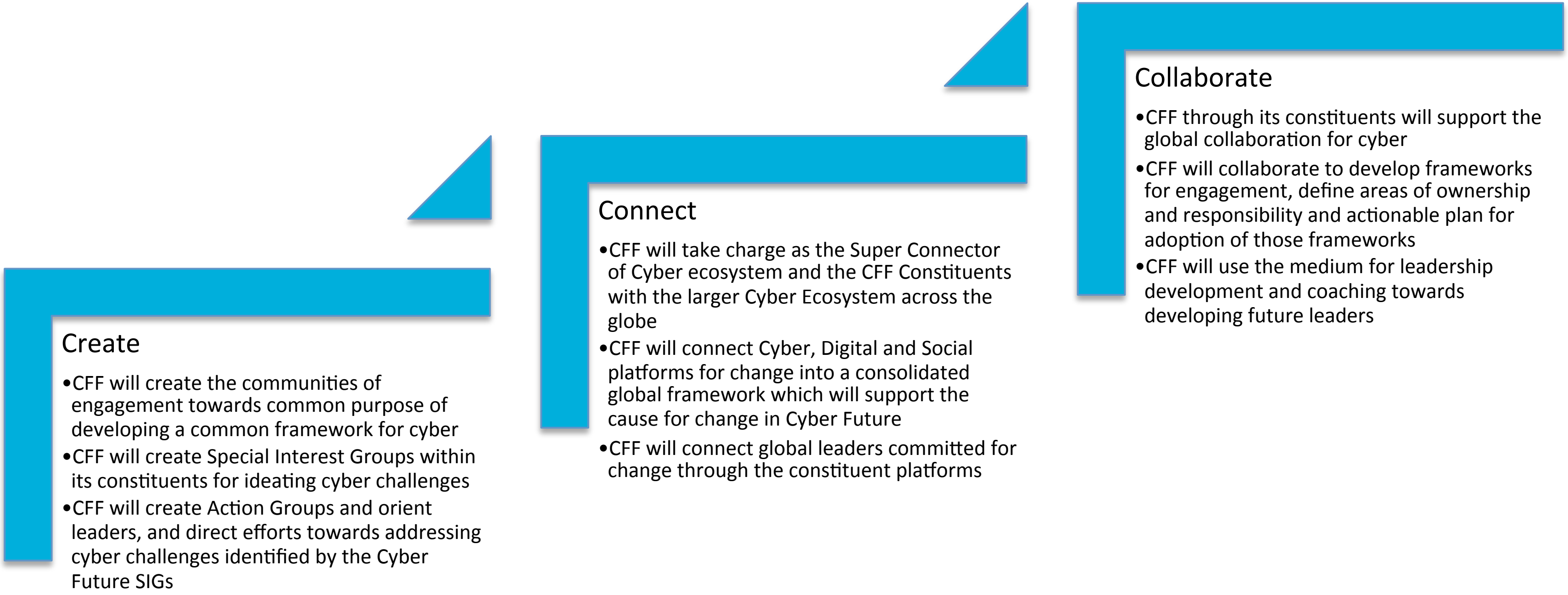
To a Collective Collaborative Global Platform of Trust and Synergy

Cyber is in a Big Mess … So What? Focus on the Solution > Trusted Global Collaboration Platform of Known Entities and Identities



- A Digital Economy needs to have a global platform for **Trusted Global Cyber Collaboration** across the triad of **Industry**, **Governments** and **Academia**
- This can be achieved **through the organization** and **communities of collaboration** acting as an **aggregate change catalyst** and action group enabling the development and adoption of Trusted Global Cyberspace

We will include Create, Connect and Collaborate our Constituents towards a Bold Cyber Future Plan that will represent



Create

- CFF will create the communities of engagement towards common purpose of developing a common framework for cyber
- CFF will create Special Interest Groups within its constituents for ideating cyber challenges
- CFF will create Action Groups and orient leaders, and direct efforts towards addressing cyber challenges identified by the Cyber Future SIGs

Connect

- CFF will take charge as the Super Connector of Cyber ecosystem and the CFF Constituents with the larger Cyber Ecosystem across the globe
- CFF will connect Cyber, Digital and Social platforms for change into a consolidated global framework which will support the cause for change in Cyber Future
- CFF will connect global leaders committed for change through the constituent platforms

Collaborate

- CFF through its constituents will support the global collaboration for cyber
- CFF will collaborate to develop frameworks for engagement, define areas of ownership and responsibility and actionable plan for adoption of those frameworks
- CFF will use the medium for leadership development and coaching towards developing future leaders

Global Challenges → Regional Breakup → Social Sectors → Economic Impact → Human Impact

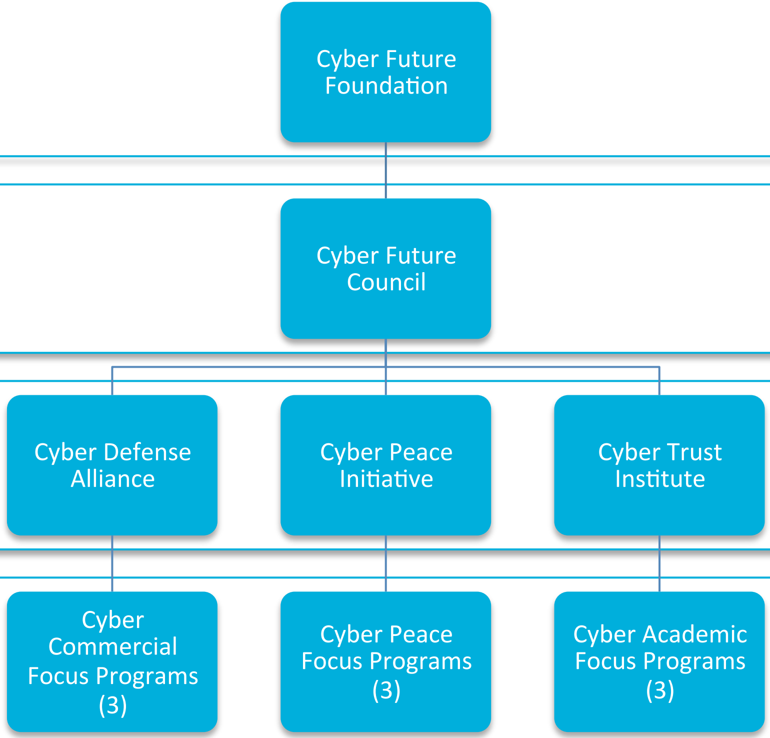
Our Constituent Organizations were built with A Unique Program Delivery Model in Mind … We will mobilize in all areas cyber

Establish the vision of Cyber Future, and sponsor the development of cyber future framework

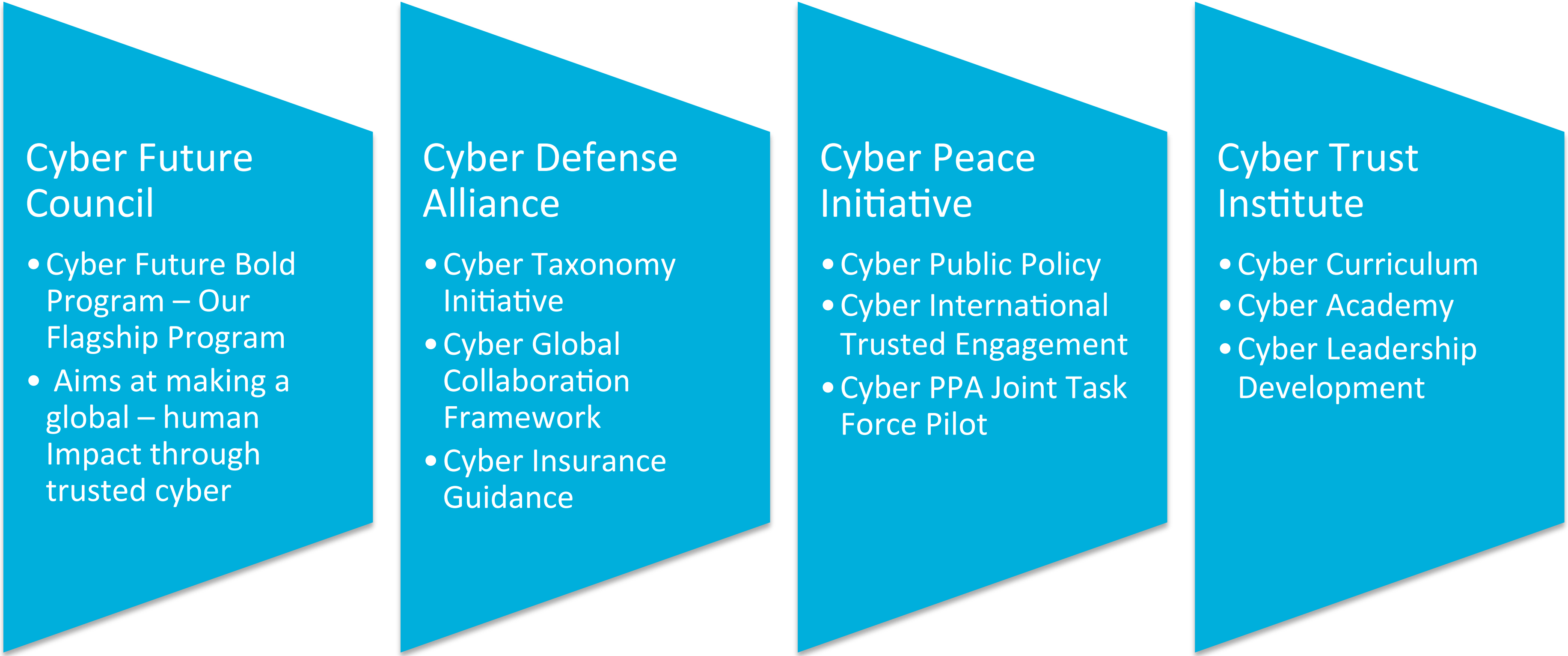
Build Cyber Future Leadership global Platform for collaboration. Support CFF Mission, Bold and Global Alliance Programs

Contribute to the development of growth of individual constituencies and their adopted missions

Initial Programs for Cyber Constituents support the foundational aspects of cyber while demonstrating our commitment of converting thought to action



We Got to do this Right … while evolving and expanding our reach and impact – we will be: Focused, Deliberate and Impactful



Cyber Future Council

- Cyber Future Bold Program – Our Flagship Program
- Aims at making a global – human Impact through trusted cyber

Cyber Defense Alliance

- Cyber Taxonomy Initiative
- Cyber Global Collaboration Framework
- Cyber Insurance Guidance

Cyber Peace Initiative

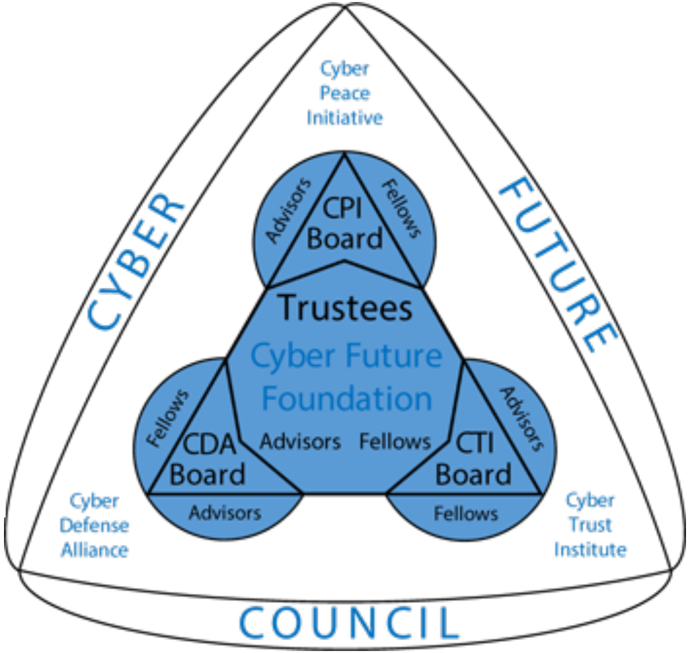
- Cyber Public Policy
- Cyber International Trusted Engagement
- Cyber PPA Joint Task Force Pilot

Cyber Trust Institute

- Cyber Curriculum
- Cyber Academy
- Cyber Leadership Development

The CFF Organization is built on Inclusiveness of Human Intellect and Diversity of Thoughts … Global Impact needs Global Reach

Global Leaders from **Every areas of society and sector** are drawn to build the Cyber Future Foundation and its Constituents



CFF is **Providing** these **Leaders** with an **action oriented platform** to effect change at the scale of Cyber through thought leadership and tangible impact

Building an Inclusive and Collaborative Global Platform for Cyber towards Supporting Global Cyber Trust Mandate – Top 10 Programs

Who	Which	Where	What	When
Val Mukherjee	CFC	Global	Cyber Future Bold Program	Q4’16-Q4‘17
Val Mukherjee	CDA	Global	Cyber Taxonomy	Q4’16-Q3’17
Harold Collum	CDA	US	Cyber Insurance Guidance & Framework	Q4’16-Q1’17
Val Mukherjee	CDA	Global	Cyber Global Collaboration Framework	Q2’17 – Q4’17
Dr. Gary Lacefield	CPI	US	Cyber Public Policy	Q3’16 – Q3’17
Val Mukherjee	CPI	Global	Cyber International Trusted Engagement	Q4’16 – Q4’17
Dave Marwell	CPI	US-TX	Cyber Private-Public-Academia Joint Task Force Pilot	Q3’16-Q1’17
Dr. Yvo Desmedt	CTI	US-TX	Cyber Curriculum	Q4’16 –Q2’17
Dr. Gary Lacefield	CTI	US	Cyber Academy	Q4’16-Q2’17
Val Mukherjee	CTI	Global	Cyber Leadership Development Program	Q1’17-Q2’17

We cannot and should not do this Alone … There is a wealth of knowledge, an ocean of organizations and an army of leaders

● COUNCIL on FOREIGN RELATIONS

IPI INTERNATIONAL PEACE INSTITUTE

EastWest INSTITUTE

● BROOKINGS

SINGAPORE INSTITUTE OF INTERNATIONAL AFFAIRS

● IISS

CSIS CENTER FOR STRATEGIC & INTERNATIONAL STUDIES
Strategic insights and bipartisan policy solutions

SWP

Think Tanks

● UNITED NATIONS

● WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Global Political & Economic

XPRIZE FOUNDATION

● Singularity University

Entrepreneurship & Innovation

ISO International Organization for Standardization

acm Association for Computing Machinery

NIST National Institute of Standards and Technology
U.S. Department of Commerce

ETSI World Class Standards

IEEE Advancing Technology for Humanity

● Standards & Academic

ISSA Information Systems Security Association

ISACA Trust in, and value from, information systems

CSA cloud security alliance®

NIST National Institute of Standards and Technology
U.S. Department of Commerce

SANS

(ISC)²®

SINET Security Innovation Network

● Cybersecurity Organizations

FORD FOUNDATION

● THE ROCKEFELLER FOUNDATION

sipri

BILL & MELINDA GATES foundation

DOCTORS WITHOUT BORDERS

unicef

THE WILLIAM AND FLORA HEWLETT FOUNDATION

Social & Humanitarian

BUILDING THE INFORMATION SOCIETY
ITU International Telecommunication Union

ICANN Internet Corporation for Assigned Names and Numbers

IMPACT INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER THREATS

NATIONAL CYBERSECURITY ALLIANCE

IETF®

● Global Cyber Organizations

● CFF Engaged in 2016

Leadership Already in Action with a Diverse Group of Founding Trustees from Social, Public, Commercial, Academic Leaders

Val Mukherjee
Founder, Chairman

Harold Collum
Founding Trustee,
Executive Director

Dave Marwell
Founding Trustee,
Vice-Chairman

William Gordon
Founding Trustee,
General Secretary

Shawn Tuma
Founding Trustee
General Counsel

Jon Shapiro
Trustee & Director
CFF

Rick Orloff
Board of Directors
CFC

Dr. Gary Lacefield
Board of Directors
CPI

Dan Talbott
Board Member
CDA

Joyce Brocaglia
Board Member
CFF

Sample Model of Engagement through CFF Platform Supporting Cyber

Cybersecurity Insurance Project Supported by Cyber Future Foundation through the Cyber Defense Alliance Initiative

Insurance companies are "shooting in the dark" when it comes to underwriting standards for cyber breach insurance policies. The Cyber Future Foundation has spent considerable time discussing this matter with representatives from some of the largest property & casualty insurance companies chartered or licensed to do business in the USA. Many of these, and most of the larger ones, not only operate within the USA, but have global operations, primarily in Europe, Asia and the Pacific Rim.

The main points of consideration, when developing underwriting standards that will conform to the NIST Cybersecurity Framework, are issues of:

- Taxonomy,
- Engineering standards,
- Competing vendor standards that are often proprietary,
- Benchmarking acceptable vendors' performance standards,
- Other such technical issues.

The Cyber Future Foundation has assembled a group of stakeholders, including some of the largest global enterprises in the cyber breach insurance underwriting category, along with carefully selected technology partners that are common to many of these organizations. We have also brought several of the largest intermediaries to the table, including third party administrators and insurance brokerage firms, to get their input into this very complex process.

Thank You

Val Mukherjee
Founder, Chairman
Cyber Future Foundation
www.cyberfuturefoundation.org
valmiki.mukherjee@cyberfuturefoundation.org
Ph: +1 (940) 337-6720

References and Credits

- http://www.dhses.ny.gov/oct/units/critical-infrastructure-protection/
- https://www.dhs.gov/ccubedvp
- https://www.dhs.gov/cybersecurity-insurance
- http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf
- 2014: A Year of Mega Breaches, Ponemon Institute, 2015 (pdf)
- 2014 Global Report on the Cost of Cyber Crime, Ponemon Institute, 2014 (pdf)
- The Cost of Malware Containment, Ponemon Institute, 2015 (pdf)
- Verizon Data Breach Investigations Report, 2013 (pdf)
- Global Corporate IT Security Risks: 2013, Kaspersky Lab (pdf)
- NCR Distinguished Professor of Law & Technology, University of Dayton School of Law, Dayton, Ohio USA. Email : susanwbrenner@ yahoo. com
- Susan W. Brenner, *Toward A Criminal Law for Cyberspace : Distributed Security*, 10 Boston University Journal Of Science & Technology Law 2 (2004).
- Brenner, *Toward A Criminal Law for Cyberspace, supra.*
- McConnell International, *Cyber Crime . . . and Punishment ? Archaic Laws Threaten Global Information* December 2000), www. mcconnellinternational. com/ services/ cybercrime. htm.
- « Cybercrime », Dictionary.com, http ://dictionary.reference.com/browse/cybercrime.
- Susan W. Brenner, *Is There Such a Thing as Virtual Crime ?,* 4 California Criminal Law Review 1 (2001).
- Brenner, *Is There Such a Thing as Virtual Crime ?, supra.*
- 18 United States Code § 2331(1).
- Tony Smith, *Hacker Jailed for Revenge Sewage Attacks,* The Register (October 31,2001), hhttp :// www. theregister. co. uk/ 2001/ 10/ 31/ hacker_jailed_for_revenge_sewa ge/.
- Bill Wallace, *Next Major Attack Could Be Over Net,* San Francisco Chronicle (November 12,2001).
- *An Argument for Anticipating Cyber-Attacks,* 2002 University of Illinois Journal of Law, Technology & Policy 1.

References & Credits

- Dan Verton, Black Ice : The Invisible Threat of Cyber-Terrorism (New York : McGraw-Hill, 2003).
- National Cyber Exercise : Cyber Storm, U.S. Department of Homeland Security (June 21,2006), http :// www. cryptome. org/ cyberstorm. pdf.
- *California Man Pleads Guilty in “Botnet” Attack,* U.S. Attorney – Western District of Washington (May 4,2006), http ://seattle.fbi.gov/dojpressrel/2006/botneck050406.htm.
- Brenner & Goodman, *In Defense of Cyberterrorism, supra.*
- Note, *Responding to Terrorism : Crime, Punishment, and War,* 115 Harvard Law Review 1217,1224 (2002).
- 18 U.S. Code § 2332b.
- “Definition of terrorism,” Wikipedia, http ://en.wikipedia.org/wiki/Definition_of_terrorism.
- “Terrorism,” Wikipedia, http ://en.wikipedia.org/wiki/Terrorism.
- *Cyberspace as a Domain in which the Air Force Flies and Fights,* U.S. Air Force (November 2,2006), http :// www. af. mil/ library/ speeches/ speech. asp ? id= 283.
- Steven A. Hildreth, *Cyberwarfare*, Congressional Research Service (June 19,2001), http :// www. fas. org/ irp/ crs/ RL30735. pdf.
- Bill Gertz, *Chinese Information Warfare Threatens Taiwan,* Washington Times (October 13,2004).
- Gertz, *Chinese Information Warfare, supra.*
- Dimitrios Delibasis, *State Use of Force in Cyberspace for Self-Defense,* 8 Peace Conflict and Development 1 (2006).
- Ian Sipress, *Computer System Under Attack,* Washington Post (October 6,2006), http :// www. washingtonpost. com/ wpdyn/ content/ article/ 2006/ 10/ 05/ AR2006100501781. html.
- Sipress, *Computer System Under Attack, supra.*
- Brenner, *Toward A Criminal Law for Cyberspace, supra.*
- John Rogin, *China Fielding Cyberattack Units,* FCW.com (May 25, 2006), http :// www. fcw. com/ article94650-05-25-06-Web.
- Brenner, *Toward A Criminal Law for Cyberspace, supra*.