OUR COMMON DIGITAL FUTURE

THE GLOBAL CONFERENCE ON CYBERSPACE JOURNAL

2017

Edited by Samir Saran

Set up in 1990, Observer Research Foundation seeks to lead and aid policy thinking towards building a strong and prosperous India in a fair and equitable world. It helps discover and inform India's choices, and carries Indian voices and ideas to forums shaping global debates. ORF provides non-partisan, independent analyses and inputs on matters of security, strategy, economy, development, energy, resources and global governance to diverse decision-makers (governments, business communities, academia, civil society). ORF's mandate is to conduct in-depth research, provide inclusive platforms and invest in tomorrow's thought leaders today.

Edited by Samir Saran

ORF OBSERVER RESEARCH FOUNDATION

CONTENTS

I see technology as a means to empower and as a tool that bridges the distance between hope and opportunity.

— Shri Narendra Modi, HON. PRIME MINISTER OF INDIA

VISION STATEMENT

Digital Identity: The Basis of Global Digital Architecture for Future

Ravi Shankar Prasad, Minister of Electronics and Information Technology, Government of India

The world is increasingly becoming digital. Internet- an extraordinary creation of human mind is no longer the monopoly of a few. Today, it is the most important tool of communication, information and is creating vast opportunities for economic development and innovation. It has given voice to the voiceless also. Therefore, the mankind has a vital stake in it. Internet being global phenomenon must have linkages with the local- local ideas and local cultures. Our view is very clear that the digital world must lead to development, empowerment and most importantly inclusive growth. Above all, it must be safe and secure, because while internet ushers promise it also causes perils at times.

On the one hand, digital technologies are allowing for unprecedented economic growth for users, communities and businesses across the spectrum.

On the other hand, these technologies have fostered the growth of malicious networks that present a real threat to our continued enjoyment of rights in a democracy. The Prime Minister of India Shri Narendra Modi has eloquently observed that cyber war is akin to bloodless war. It is in this connection that India's initiatives of safe and secure digital identity with extraordinary Aadhaar programme based on home grown safe, secure and low cost technology merits special mention. As such, nations have had to respond dynamically to adapt to those changes brought about by the digital world, whether they have to do with the economy, national security or very simply, the way we communicate. However, few have succeeded in remaining agile and crafting a sustainable digital economy.

The key to capturing the opportunity and mitigating the risk brought about by the digital realm lies with the individual: through her identity.

The key to capturing the opportunity and mitigating the risk brought about by the digital realm lies with the individual: through her identity. Identity is a central component of all transactions today. Without identity, individuals struggle for a sense of belonging in the community, economy or broader democratic polity. In some cases, a sense of misplaced identity can even foment radicalization and extremism, especially in digital spaces. The importance of identity has even been highlighted in the UN's Sustainable Development Goals, which call for the provision of a legal identity for everyone by 2030. India as a nation was quick to recognize the significance of identity as a positive reinforcement, and, thus, went on to create the most successful digital identity in the world – Aadhaar.

India's journey with Aadhaar offers important evidence on how identity can help catalyze the growth of the digital economy, form the basis of national security, and help in the delivery of social benefits. Additionally, it offers a template for a cost-effective digital ecosystem which other countries can emulate. Most impor-

tantly, it highlights the centrality of identity within the global digital architecture of the future.

An important distinction in the Aadhaar initiative led by Prime Minister Narendra Modi is that now there is a robust law duly passed by the Parliament which creates a very salutary provision of safe and secure digital identity process and also respects privacy of individuals.

The Identity-based Digital Economy

Few years ago, India was faced with a conundrum. Over half its constituents had no way of proving their identity. This precluded their participation in the formal economy, as one cannot open a bank account, access credit systems, or acquire insurance without a personal identification document. Additionally, the inability to identify half the population made the delivery of government services exceedingly tricky. Aadhaar was conceived to solve these issues by creating a unique digital identity for individuals based on their biometric data. Today, it boasts 1.18 billion enrolments, giving India the most significant digital identity footprint in the world.

Far reaching transformational programs like Digital India, Make In India, Skill India, Startup India are all technology driven programs for transformation and empowerment of ordinary Indians designed to usher in greater access to avenues of development. Banking the unbanked, securing the unsecured, funding the unfunded, taxing the untaxed and giving voice to the unheard are all being made possible through verifiable digital identity.

Aadhaar underpins a host of innovative applications that have transformed the working of commerce in the country. The first is the Aadhaar-Enabled Payment System (AEPS), which allows customers access to their Aadhaar-linked bank accounts through Aadhar authentication. The AEPS has brought about financial empowerment at the grassroots level through the deployment of micro-ATMs. The service allows for deposits, cash withdrawals, and fund transfers. The second is the Aadhaar Pay application which uses an individual's biometric information to authorize payments to merchants.

The third is the India Stack, an open Application Programming Inter-

face for developers that uses Aadhaar as the basis for verification, an e-KYC digital locker for the safe deposit of documents, has an e-signature feature, and a Unified Payments Interface for financial transactions. India Stack makes a user base of over 1 billion people available to start-ups and entrepreneurs who wish to build applications on top of it to integrate parts of their businesses or create new services from scratch. India Stack makes cashless, presence-less, and paperless service delivery ecosystem possible. Now, a fruit seller can avail of an intra-day loan and pay it back the same day through her mobile phone without having to waste time by visiting a bank.

In today's world, data is the most valuable resource for an economy. Aadhaar has created an opportunity for India and its citizens to utilize this resource to advance the domestic digital economy and grow it to USD 1 trillion within the next five years.

Using Identity to Fight Terrorism

Terror requires financing to operate. In the absence of funding, equipment, supplies, people and resources cannot be purchased or attracted. The sources of capital may be legal or illegal, with money being transferred in small amounts rather than large lump sums. Terror financing is a global phenomenon that threatens a state's security and economic stability.

The internet has been an important tool for terror financing. It offers both terror groups and their donors broad reach, efficiency, and most importantly, anonymity. With access becoming easier every day, the internet is a powerful weapon for outreach. Billions of individuals flood social media and other popular websites. These channels allow terror organizations to effectively launder money, raise funds directly, and recruit new members. Additionally, terror groups are drawn to the internet because it offers them allows them to avoid detection.

This is where identity comes in. Aadhaar snatches away the anonymity that shelters evil activities. The linking of Aadhar to bank accounts, Permanent Account Numbers (PAN), and mobile phones has been instrumental in stemming the tide

of black money and terror financing in the country as it has limited the ability of individuals to launder money and transfer funds for illicit activities through these channels. Illustratively, over 1 million fake PAN cards have been cancelled as a result of the linkage of Aadhaar with PAN numbers. Additionally, because Aadhaar requires the use of biometric information for authentication and registration, it cannot be duplicated. Thus, it is impossible to create duplicitous Aadhaar cards.

Identity-based Social Welfare

Countries spend billions on social welfare programs, but these schemes are difficult to implement and plagued with leakages. One limitation in the effective implementation of these programs is the dearth of adequate financial infrastructure to facilitate transfers to the intended beneficiaries. This leakage of funds can be as high as 70 to 85 percent. An identity-based payments system helps overcome this issue by allowing governments to identify beneficiaries and transfer welfare directly to their accounts correctly.

In this regard, the implementation of the Aadhaar-based Direct Benefit Transfer scheme has saved the exchequer INR 50,000 crores over the past three years. Aadhaar has made the delivery of social welfare programs like the National Rural Employment Guarantee Scheme (NREGS) and Social Security Payments (SSP) more efficient and timely. Ration cards were typically bound to one Public Distribution System outlet, regardless of how poor its services were. With Aadhaar, ration customers can avail of the services of any PDS outlet. Illustratively, in Andhra Pradesh's Krishna district, PDS outlets can no longer give their customers a poor deal, for fear of loss of business to better quality vendors.

The Future: An Identity-based Global Digital Architecture

Within a short period, the implementation of Aadhaar has propelled India to the centre of the global digital story. It has spurred the growth of India's digital economy, fostered financial inclusion and distribution of social welfare, and safeguarded the country from external and internal threats. In this regard, Aadhaar has

realised many of the goals identified in the global cyberspace conferences incubated by the London process.

Aadhaar has shown that genuine innovation need not be complicated or expensive. It has proved that governments can provide cost-effective, quality digital infrastructure. Lastly, it has established the profound importance of identity to the broader global digital narrative of tomorrow. Around the globe, 4.4 billion individuals are yet to come online. Aadhaar has shown that giving them a digital identity is the first step in this regard.

Aadhaar is a data-driven innovation that serves as a blueprint for other nations. Several countries such as Morocco, Russia, Algeria, and Tunisia are already contemplating India's model for their own. Moreover, international organizations like the World Bank are looking to use Aadhaar as an archetype to structure similar strategies in other parts of the world.

Identity will be the cornerstone upon which the global digital architecture of the future is built. The sheer scale of digital transformation happening in India, touching the lives of ordinary people in a population of more than 1.3 billion is going to be a great beacon for the developing world. India, for its part, will help see this through by guiding the rest of the world through this journey.

EDITOR'S NOTE

Our Common Future

Samir Saran, Vice President, Observer Research Foundation

For a medium considered to have revolutionised communications, it is ironic that the many struggles around the governance of cyberspace stem from a lack of communication – communication among states, between states and citizens, and between those that create technology and those that consume it. Normative processes that will determine the future of cyber governance have greatly benefited by bringing together actors who represent diverse geographical, political, economic and social realities. One of the most important among these processes is the Global Conference on Cyberspace (GCCS).

Conceived in London in 2011, the GCCS is the largest gathering of all stakeholders on cyberspace issues. It has already managed to bring into this fold key interlocutors from government, civil society, industry and academia. The fifth edition of the conference, convened by India, is a significant landmark in the evolution of the London Process. GCCS 2017 is the first time that the gathering is hosted by a non-OECD economy. This very fact leads to an opportunity for the

internet community to engage with a wholly new demographic and different set of issues animating the next billion internet users. That India hosts this process now is a message in itself and augurs well for greater degree of pluralism in the agenda, grammar and ambitions of this process.

This idea is reflected in the four main pillars for GCCS 2017 – inclusion, growth, diplomacy and security. This volume of essays captures some of the critical debates on these issues from foremost leaders, visionaries, founders and young minds in technology, policy and governance. While previous editions of this conference have been designed as high-level stocktaking exercises, this edition has the potential to go a step further and create an independent norm-setting initiative led by diverse and emerging economies. The essays in this volume are intended to guide this endeavour.

The multiple goals of policymaking -- providing access, securing the medium and spurring economic activity — are no longer mutually exclusive.

The multiple goals of policymaking — providing access, securing the medium and spurring economic activity — are no longer mutually exclusive.

These are all interlinked interests. There is perhaps no better example that is more illustrative of this phenomenon than the opportunity presented by digital payments. Digital payments have immense potential in promoting financial inclusion to those at the bottom of the pyramid and in banking the unbanked. It can enable micro entrepreneurship and serve as the backbone for services in the digital age. At the same time, digital transactions have sometimes come under the shadow of technological vulnerabilities and in the unsafe practices of users who make them. Governments today have to juggle policy priorities that are often at odds with each other -- providing access cannot ignore concerns around security and securing the medium cannot come at the cost of stifling innovation. Reconciling these challenges in pursuit of one goal is the digital trilemma for cyberspace policymakers today.

Addressing these challenges will require policymaking that is both technologically and socially dynamic. It will require normative guidance that is targeted and yet inclusive. With formal multilateral processes such as the UN Group of Governmental Experts on Developments in the Field of Information and Communication Technologies ending in a lack of consensus this year, initiatives such as the GCCS assume more importance. The conference can serve as a forum to make the global discourse around cyberspace more representative and plural – this year we will witness some of the normative conversations begun by bodies like the Global Commission on the Stability of Cyberspace and have these ideas deliberated upon.

The essays in this volume, covering a range of topics from cyber conflict to digital connectivity, aim to bring a diversity of interests and perspectives on to the same table, in the hopes that they will guide discussions for future gatherings and maybe even answer some of the long contested issues for policymakers today.

Asia is not only home to the largest number of internet users in the world, it is also poised to lead the world in technology, innovations and regulatory policy - it is therefore only fitting that GCCS 2017 is being stewarded by India. The process will benefit from the democratic ethos of policy conversations in India and will allow voices that have remained on the sidelines to have their chance to shape our common digital future.

FOREWORD

From London to New Delhi: Building an Open, Secure Internet for All

BORIS JOHNSON
Secretary of State for Foreign and Commonwealth Affairs, United Kingdom

ON 12 MAY, hospitals across Britain were struck by a ransomware attack known as WannaCry. As our National Cyber Security Centre (NCSC) began its emergency response, reports of similar incidents started coming in from across the world. In Spain, telecoms companies were hit; in India, various police forces fell victim; in Germany, it was transport and railways that suffered; in Russia the interior ministry was infected. It soon became clear that over 100 countries had felt the effects of WannaCry, demonstrating the global and indiscriminate nature of this threat.

Here in Britain, the NCSC's experts helped our National Health Service to get back to normal – although the situation would have been worse if hospital staff had not reverted to manual systems. While the WannaCry attack was not the 'Cy-

ber Armageddon' that some have predicted, the fact that this ransomware spread like wildfire – and ruthlessly exploited old and unpatched software – exposed the policy problems created by this kind of threat. Put simply, borders are irrelevant and no government can protect its people in isolation.

"Cyber" is derived from kubernetes, the Greek word for "steersman". How should we steer ourselves across the uncharted waters of the digital age? The UK was the first to host this conference in 2011, and our shared aim must be to agree common principles for behaviour within and between states in the digital age. International law applies online as it does offline – and so too should the conventions that guide our behaviour in other aspects of life. To this end, the UK is developing a Digital Charter with the aim of agreeing how people and businesses should behave online in order to create an environment for societies and economies to flourish.

But the challenges never stand still. All around us, new trends are evident, from cyber-enabled interference in democratic elections to the spread of terrorist propaganda across the internet, even as the groups themselves lose control of real territory. Meanwhile, criminals make increasingly sophisticated attempts to separate ordinary people from their money. Espionage, propaganda and theft are as old as humanity, but today they occur on a huge scale – and at lightning speed – when carried into cyberspace.

> We are all stronger when we share knowledge, improve our cooperation and invest in each other's capabilities.

Hence the necessity of creating a secure Internet, where people and data are properly protected. This does not mean sacrificing human rights for the sake of security – the two can and should go hand-in-hand. It does mean ending impunity for malicious actors, developing networks that are secure by default and ensuring that basic precautions are universal. Despite episodes like WannaCry, many attacks succeed using relatively primitive techniques. The vast majority of incidents reported in the UK could be avoided with safeguards as elementary as installing new security patches, or updating

default passwords.

Cyberspace also challenges our traditional ideas of legal jurisdiction. Data about one country's citizens can be subject to the laws of another simply because of where it is physically stored. Those represented at this Global Conference on Cyberspace will hold different views on how to respond: that is precisely why we need to talk.

We are all stronger when we share knowledge, improve our cooperation and invest in each other's capabilities. In this spirit, I am delighted that this year's conference will agree a Global Agenda for Cyber Capacity Building.

One of the greatest debates of our time is how to create a free, open and secure cyberspace for the benefit of all. You are the steersmen charting our way through this extraordinarily complex labyrinth – and I wish you every success.

For a Free and Secure Global Internet

Federica Mogherini, High Representative of the European Union for foreign and security policy, and Vice-President of the European Commission

The internet has been a global force for human development, since the early days of its inception. It has offered opportunities to learn, to reach new markets, to innovate. In a world of growing inequalities, access to the internet is the key for marginalised communities all over the world to grow, study and connect.

Yet, in recent times, we are all increasingly aware of the threats running on the web: cyber-attacks have too often made the news; our defence systems cannot ignore the possibility of cyber-warfare; and too many of our young people have been exposed to the online propaganda of terrorist groups.

Cyberspace is a global common, and we all share an interest to keep it safe. I am convinced that cyberspace can be at the same time safe and open, and that the opportunities of global connectivity outnumber its dangers, by far. If we want to preserve and expand these opportunities, we must also invest in the security and the governance of

our cyberspace.

For this reason, we Europeans believe that international cooperation must be the main path to "promote a free and secure global internet" – in the words of our Global Strategy for foreign and security policy, which I presented last year. The European Union is actively contributing to the capacity of our international partners to fight cybercrime and address cyber threats: we have launched global capacity building programmes to promote the rule of law in cyberspace, training law enforcement officials to investigate and prosecute cybercrime. With our Global Strategy, the European Union has committed to engaging in cyber diplomacy and to seeking international agreements on responsible behaviour in cyberspace, based on existing international law. A global framework on cyber security is an integral part of our efforts to build a stronger global governance, and a more cooperative world order.

Cyber-insecurity transcends national borders by definition: joining forces among countries is crucial to effectively address this challenge.

This is a view we share with India: at last month's EU-India Summit in New Delhi we jointly reaffirmed that international law is applicable in cyberspace, and that there is "a need to continue and deepen deliberations on the applicability of international law to cyberspace and set norms of responsible behaviour of States."

While we work at better global cyber-rules, we must also tackle the immediate cyber-threats that already have an impact on our citizens' lives. Cyber-insecurity transcends national borders by definition: joining forces among countries is crucial to effectively address this challenge, and the European Union's institutions and Member States are stepping up cooperation in this field.

To protect our cyberspace, we need better capabilities, more research, more training and exercises on how to respond to an attack. In the last few months we have already set up a number of new initiatives and structures with a focus on

cyber-security. Last year we signed a Joint Declaration for cooperation with NATO: out of 42 common actions we have agreed upon, seven cover cyber-security issues. We inaugurated a European Centre for Countering Hybrid Threats in Helsinki, under the leadership of Finland and other Member States. The European Defence Agency, which I lead, is working on a European Cyber Defence Training and Exercise Platform. And just two months ago, the European Commission has proposed to create an EU Cybersecurity Agency: the Agency would support our Member States to prevent and react to cyber-attacks, but also put in place an EU-wide certification framework to ensure that products and services are cyber-secure.

Over the last year, the European Union has taken unprecedented steps to improve cooperation among its Member States on defence issues. Many of the initiatives we have launched – such as the Permanent Structured Cooperation on defence, the Coordinated Annual Review of national defence budgets, and the European Defence Fund – provide us with great opportunities to research and develop new capabilities for cyber-security, in a more cooperative and efficient manner.

We are also getting ready to respond to cyber-attacks through our foreign policy tools, including economic sanctions. In June 2017, with the European Union's ministers of foreign affairs, we decided to develop a so-called Cyber Diplomacy Toolbox, that is, a blueprint for a joint EU diplomatic response to malicious cyber activities.

Beyond the risk of attacks against our critical infrastructure and our data, there is another security issue linked to the internet, more subtle, which we cannot ignore. Terrorist groups like Daesh have used the web to spread their lies, radicalise and recruit all around the world, from Europe to South Asia. Their propaganda needs to be confronted first and foremost by taking down the illegal contents from the internet. To address the issue of the accessibility of terrorist materials, the European Commission has established an Internet Referral Unit within Europol, the European agency for police cooperation. The Unit actively scans for terrorist content online and

then refers it to the relevant internet companies – such as Google or Facebook. In just a couple of years, the Unit has already referred tens of thousands of pages. And in 90 per cent of cases, the internet companies have removed the material.

If we want our internet to be truly safe, what is illegal offline must also be illegal online. At the same time, all the freedoms and the inalienable rights that we, as the European Union, cherish and protect must also be guaranteed on the internet. In recent years, we have seen tough penalties against bloggers, laws to criminalise legitimate dissent on social media, internet shutdowns. We must call things by their name: these are violations of human rights, crimes against free speech. And the European Union will always side with the victims, working to protect them and to restore their freedoms.

The cyberspace can only be free if it is secure, and can only be secure if it is free. This is what we Europeans believe, and this is also the spirit of the Global Conference on Cyberspace. We share your goal of "A Secure and Inclusive Cyberspace for Sustainable Development". And we, as the European Union, are ready to engage with all those who share this goal – in our partner countries, in the civil society and in the business sector. Together we can find innovative and cooperative solutions to make the internet a true force for good, free and secure for all mankind.

A Southeast Asian Perspective Towards Cyber Norms in a Post-UNGGE World

Yaacob Ibrahim, Minister-in-charge of Cyber Security, Singapore

The 2016/2017 United Nations Group of Governmental Experts (UNGGE)'s inability to reach consensus was a setback, but we should not let this deter our joint efforts to implement a set of international cyber norms. The world needs these norms more than ever, given how digitalised and connected we are, and in response to the common scourge of cyber threats. Singapore remains deeply committed to such efforts, and will continue to work with our regional and international partners to realise this shared objective.

Why Cyber Norms Matter to Us

Singapore fully supports the development of international cyber norms. As a small city-state, Singapore relies on clear "rules of the road" that apply to all countries, big and small. We are also one of the world's most connected cities; each Singaporean has almost two handphones on average, and our national broadband infrastructure is the

world's fastest[1]. While our high quality digital infrastructure has catalysed our economy and improved our quality of life, it also makes us vulnerable to cyber-attacks.

Singapore is also located in the centre of one of the world's fastest growing regions, Southeast Asia. Southeast Asia has a population of more than 600 million people – larger than the European Union – and has one of the fastest-growing middle classes in the world, with more than 200 million people expected to join the middle class by 2020. This economic and demographic dividend will boost demand for greater connectivity and digitalisation, which in turn will drive the Association of Southeast Asian Nation (ASEAN)'s digital economy. A safe and trustworthy cyberspace is thus an enabler and an imperative for Southeast Asia's economic prosperity.

The rapid pace of digitalisation in Singapore's domestic and regional environments makes it more essential to secure our cyberspace. After all, cyber-attacks are not a theoretical threat. Earlier this year, the IT networks of two universities in Singapore were found to have been breached by Advanced Persistent Threat actors, possibly to steal information related to government or research. In early November 2017, regional threat actors also compromised the websites of ASEAN and other government agencies in Southeast Asia.

> Together with our regional and international partners, we will continue our efforts to champion the adoption of cyber norms – through promoting more dialogue, developing informal regional norms, and catalysing practical cooperation – to build a safe and trustworthy cyberspace for all.

These developments underscore the need for a consistent set of rules or norms for all states and stakeholders in cyberspace, so as to build a safe and trustworthy cyberspace for all.

Building on the Work of the UNGGE Through Multiple, Complementary Fronts

Singapore believes that the UN must

continue to play an important role in moving international discussions on cybersecurity issues forward. It is only at open and inclusive platforms such as the UN that all states, especially small ones like Singapore, can have an equal stake and an opportunity to shape the global discourse on a rules-based international order for cyberspace.

That is why Singapore fully supports the work of the UNGGE, even though we are not a member. The recent UNGGE process has shown that consensus across the broad international community may be difficult to achieve, given the diverse circumstances between countries and regions. But this should not hold us back. It remains important to build on the UNGGE consensus report in 2015 – which set out 11 voluntary norms of responsible state behaviour in cyberspace – through international and regional dialogue, to operationalise the UNGGE's recommendations.

Singapore and other states must, therefore, strive to raise awareness and applicability of the UNGGE norms, through regional and inter-regional conversations that can complement the UN process. Groupings such as the Organisation of American States, the European Union and ASEAN play an important role in contributing to a broad-based conversation on cyber norms.

To this end, Singapore is playing an active role in Southeast Asia to move the conversation on cyber norms forward. We do so in three ways: promoting more dialogue, developing informal regional norms, and catalysing practical cooperation.

Promoting More Dialogue

First, Singapore believes that dialogue is essential to focus the attention of the international community on key cyber issues.

To facilitate greater dialogue among senior government officials in the international community, Singapore hosts the annual Singapore International Cyber Week (SICW). The 2nd SICW was held in September 2017, and provided a platform for more than 7,000 stakeholders, including policy-makers, industry experts and non-governmental organisations, to forge partnerships and engage in critical dialogue on salient issues in cybersecurity. The International Cyber Leaders' Symposium, for example,

featured a robust panel discussion between thought-leaders from government and industry on the challenges in implementing norms of responsible cyber behaviour. It is through such dialogue that we have a better appreciation of each other's perspectives and challenges, and thus the basis for developing effective norms and embarking on practical cooperation.

Developing Informal Regional Norms

Second, Singapore has also been working with our regional partners to develop and implement a set of informal regional cyber norms, which are congruent with the 2015 UNGGE norms.

Developing regional norms is no easy feat in Southeast Asia, given the differences in digital maturity, cyber capabilities, and policy challenges. Nonetheless, ASEAN's 50-year history of mutual cooperation has enabled member states to embrace the task of developing cyber norms with confidence and trust.

That is why collaboration between ASEAN members on cyber issues has been encouraging. For instance, at the inaugural ASEAN Ministerial Conference on Cybersecurity (AMCC) hosted by Singapore in October 2016, ASEAN Ministers and the ASEAN Secretary-General agreed on the importance of forging closer ASEAN cybersecurity cooperation in the areas of cyber policy coordination, capacity-building and cyber norms of responsible state behaviour. At the 2nd AMCC in September 2017, participants agreed that it was important to establish international voluntary cyber norms of responsible State behaviour as the foundation for a rules-based cyberspace. Regional platforms such as the AMCC reflect Singapore and the region's commitment to work together, to enhance regional cybersecurity discussions and cooperation.

Catalysing Practical Cooperation

Finally, Singapore recognises that dialogue and norms must be complemented by practical cooperation. After all, technical capabilities, resources, and access to information affect a state's ability to respond effectively to cyber threats. Practical cooperation also hones capabilities, and builds confidence among like-minded partners. These in turn cultivate an environment of mutual trust with one another.

Singapore has leaned forward to facilitate regional cyber capacity-building efforts and confidence building measures (CBMs). For example, Singapore launched a S$10 million ASEAN Cyber Capacity Programme (ACCP) to develop technical, policy and strategy building capabilities within ASEAN, and with international organisations such as the UN Office for Disarmament Affairs (UNODA).[2] Under the auspices of the ACCP, Singapore has launched initiatives such as the ASEAN Cyber Norms workshop, and announced plans for an ASEAN Cybersecurity Industrial-Attachment Programme (CS-IAP), which would provide participants with training on the operations and management of Security Operations Centres.

Taken together, the cultivation of capacity-building and CBMs effectively complement ongoing discussions on cyber norms, to create a mutually reinforcing "virtuous triangle" that aligns the interests of states, and fosters greater trust and collaboration in cyberspace.

The Way Forward in a Post-UNGGE World

I hope Singapore's experience proves useful in navigating a post-UNGGE world. It is heartening to note the interest across the various stakeholders to sustain discussion on the adoption of voluntary cyber norms. Regional conferences such as the GCCS also play an important role in taking the conversation on cyber norms forward.

As Southeast Asia continues its digital transformation journey, Singapore remains firmly plugged into this global conversation. Together with our regional and international partners, we will continue our efforts to champion the adoption of cyber norms – through promoting more dialogue, developing informal regional norms, and catalysing practical cooperation – to build a safe and trustworthy cyberspace for all.

[2]For example, Singapore has agreed to provide sponsorship for the UNODA Flagship Online Training Course on the Use of ICTs in the Context of International Security.

Cyberspace: A Force for Good, If Governed by the Rule of Law

Halbe Zijlstra, Minister of Foreign Affairs, The Netherlands

Back in the early years of the 17th century, when Dutch lawyer Hugo Grotius laid the foundations for modern international law, no one could have guessed that one day, its scope would have to be extended into new, exotic and unimaginable domains. After starting in the naval sphere, it soon reached the skies with the advent of the aeroplane. And now, in our 21st century, it is entering a new and elusive dimension: cyberspace.

The word 'cyberspace' itself first appeared in 1984, in the cult classic science fiction novel Neuromancer. When author William Gibson coined the term, he said something which still rings true today:

> *"Cyberspace is not good or bad. Modern techniques are morally neutral – until we apply them."*

Indeed, in recent years, cyberspace has proven to be a powerful force for good. In many countries around the world, cyberspace has provided an innovative boost and brought impressive economic growth.

The gains of cyberspace are not equally distributed. With 60 percent of the world population still having no access to the internet, there is a huge global connectivity gap.

The digital economy accounts for 7.7 percent of the total Dutch economy, a number which is rapidly growing. The digital world is now more important to the economy than Amsterdam's Schiphol Airport and the Port of Rotterdam combined! Bits and bytes have come to outweigh Boeings and boats.

In other countries, the digital economy is reaching similar levels of importance. Take India: a major cyber power with a well-deserved reputation for its innovative, world-beating IT sector. Here, the cyber sector contributes strongly to India's staggering seven percent growth.

But, as with every technological innovation, there is a downside.

First, growing digital dependency creates new vulnerabilities and risks. Not only to criminals, who prey on our citizens and companies. But also to hostile states, who use cyber operations for espionage, disinformation and military gain.

Second, the gains of cyberspace are not equally distributed. With 60 percent of the world population still having no access to the internet, there is a huge global connectivity gap.

If we want cyberspace to remain a force for good, these are issues we need to urgently address.

Governments cannot do this alone. Other parties need to step in as well. Cyberspace belongs to everyone and to no one. But ultimately, we all share the same interests.

This is why, in 2016, we launched the Global Commission on the Stability of Cyberspace, the only forum where government, industry, technologists and civil society are joining forces to reach a common goal: a digital future in which the fruits of an open, free and secure cyberspace are there for all to enjoy.

Most importantly, at the Global Conference on Cyber Space, we discuss ways to deal with the vulnerabilities and risks I mentioned earlier.

Challenges that risk turning cyberspace into the opposite of a force for good. A jungle by night, where might makes right, and the perpetrators of attacks cannot be held to account.

The existing body of international law, which has long underpinned relations between states, applies equally in cyberspace.

Preventing this is in all our interests. And here, the key to success lies in clear rules, which apply to everyone equally.

This may sound horribly complicated. But the good news is that we don't need to develop anything new. These rules are readily available.

We believe, as do many other countries, that the existing body of international law, which has long underpinned relations between states, applies equally in cyberspace. And it provides the best guarantees for maintaining an open, free and secure cyberspace, where human rights are protected, making it a universal force for good.

Of course, the question is, how does international law apply to this new dimension?

This is the heart of the matter, and it is something that must be actively debated at conferences like this.

Various initiatives in this area have already been launched. The United Nations' Group of Governmental Experts process made important headway with its 2013 and 2015 reports. India has played an important and constructive role in this process. We should all build on the important progress that has been achieved.

The Tallinn Manual 2.0 and the Hague Process are other useful examples, providing guidance on how to apply long-established legal principles in the cyber domain, such as sovereignty, non-intervention, due diligence and state responsibility. But also on the law applicable to the use of force and international humanitarian law. And, most importantly, they help shed light on the legal framework surrounding cyber operations that don't meet the threshold of an armed attack.

Take, for instance, a situation where foreign (state-backed) hackers meddle in elections. Or where

they compromise bank accounts or citizens' private data. Or when they disrupt a country's electricity supply. What legal options does a victim state have with which to respond? Many of these cyber operations are clearly malicious. They may even rise to the level of an internationally wrongful act, but at the same time fall short of what can be defined as an armed attack.

We need to resolve these questions. And we need to do so urgently. Because in recent years, tensions and outright hostility among states has been on the rise. Cyber incidents have occurred with increasing frequency. In the meantime, the mood in the international debate at UN level on stability in cyberspace has soured – at the very moment we need it the most.

For me, this all serves to underscore the importance of the GCCS process.

That is why it's so important that this conference works to move the discussion forward. With all stakeholders: nation states, the tech community, companies, non-governmental organisations and academics, and so on. Together, under the able leadership of India – one of the key emerging economies and great powers of the 21st century—we must now take the next steps.

We are very grateful for India's willingness to host this year's edition of the GCCS, and we feel confident in passing the baton. India is uniquely positioned to broaden the GCCS agenda to take in issues regarding equitable development and digital inclusion. It is worth remembering that not all countries are at the same level of economic development. And the same holds true in the digital domain. In order to tackle the digital divide, we have set up the Global Forum on Cyber Expertise (GFCE), investing in capacity-building in developing countries, thus helping them keep the internet open and free.

As co-chairs, the Netherlands and India are collaborating on an agenda in which economic growth, digital security and online freedom go hand in hand; Cyber4All, as this year's theme of the GCCS aptly puts it. With many of the next 500 million internet users coming from India, it makes perfect sense for India to take the lead.

Let's all work together towards our common goal: a safe and secure cyberspace where clear rules apply to all. A cyberspace that is governed by the international rule of law. A cyberspace of which our national hero, Hugo Grotius, would undoubtedly approve: a universal force for good.

Developing a New Humanitarian Response in the Area of Cyberspace

Peter Maurer, President, International Committee of the Red Cross

We are living in a rapidly changing world, where technological advances and digitalization are occurring at an ever-faster pace.

Technology is creating profound changes in service delivery, triggering new partnerships and innovations. In India, for example, information technology has been used successfully to reach poorer sections of society by linking their mobile-phone services and government-issued IDs to their bank accounts, so that government subsidies can be delivered directly to beneficiaries.

The International Committee of the Red Cross (ICRC) has also been affected by this global digital transformation, which has significantly altered the environment and manner in which we operate. This shift offers both opportunities and challenges in terms of how we respond to increasing humanitarian needs.

First, improved analysis of external data enables the ICRC to better anticipate,

understand and respond to humanitarian crises. We can achieve this through big-data analytics and evidence-based analysis of specific situations or more global trends.

Second, cyberspace offers the ICRC greater opportunities to engage digitally with people in need and facilitates our access and response to them. Similarly, digital connectivity with beneficiaries and other key stakeholders – including parties to armed conflict – can be extremely useful when movements are limited by the security situation, or simply because people prefer to engage with the ICRC this way.

Cyberspace also allows beneficiaries to be involved in the design of responses to their needs, methods to recover their livelihood and ways to enhance the well-being of their communities. This direct input and feedback allow the ICRC constantly to adapt its response to the prevailing needs.

However, digital proximity will never fully replace our presence on the ground.

Direct contact with people and communities is key to how we operate and is often the only way we can respond to certain specific humanitarian needs. This is all the more true in the case of those who do not have access to cyberspace and so could be the most vulnerable of all.

Third, the ICRC is always looking for opportunities to use technology to provide new types of services or improve existing services in response to beneficiaries' changing needs. The ICRC is pioneering the use of cyberspace in its work to locate and reconnect people separated during crises. As far back as the 2004 tsunami and, more recently, during the 2015 Nepal earthquake, we offered survivors satellite phones and an internet platform to help them re-establish contact with their loved ones. Today, we continue to explore how to harness the potential of new technology to improve our humanitarian response on behalf of those in need.

The ICRC also relies on remote-sensing technology in its efforts to protect civilians from the effects of hostilities. For example, as part of our work around Mosul, Iraq, toxic industrial chemical installations were mapped using a combination of satellite imagery and specialized

Asserting that cyber warfare must respect the rules of IHL is by no means an encouragement to militarize cyberspace, nor does it legitimize cyber warfare.

internet search engines, among other. Where possible, we subsequently used this information in our dialogue with parties to the conflicts in the area on the obligation to take all feasible precautions to protect the civilian population from the effects of hostilities.

Protecting Humanitarian Data

Digitalization has also led to a tremendous increase in the number and diversity of ICRC data, and we are keenly aware of the various privacy and security risks this entails. The ICRC, like all organizations, could fall victim to a cyber attack – something that could ultimately affect the delivery of humanitarian services. Beneficiaries might unwittingly expose themselves to unwanted consequences when they use insecure digital platforms to avail of humanitarian services, or if the data is then used for other purposes.

The ICRC works continuously to strengthen protection of the data it generates or gathers, in line with the organization's robust data-protection framework and standards, and conforming to the "Do No Digital Harm" maxim. In fact, the ICRC is taking the lead in the humanitarian community in terms of reflection on the protection of personal data.

Cyberwarfare and International Humanitarian Law (IHL)

The ICRC's role, as the guardian of IHL, is to reaffirm the protection afforded by this legal framework that seeks to limit the effects of armed conflict. IHL protects people who are not or are no longer participating in hostilities and restricts the means and methods of warfare - including digital - that belligerents can use. As in the case of any new weapon, it governs the use of cyber military capabilities. There is no legal vacuum in cyberspace.

The ICRC understands "cyber warfare" to mean operations against a computer, or a computer system,

through a data stream, when used as means and methods of warfare in the context of an armed conflict. In this respect, the ICRC is pleased that the 2013 and 2015 Reports of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunication in the Context of International Security confirmed that "international law, and in particular the Charter of the United Nations, is applicable" and noted "the established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction".

Asserting that cyber warfare must respect the rules of IHL is by no means an encouragement to militarize cyberspace, nor does it legitimize cyber warfare. Any resort to force by States, whether physically or via cyber space, remains subject to the provisions of the UN Charter (jus ad bellum). The key point, however, is that – in addition to, and independently of, the requirements under the UN Charter – the limits imposed by IHL govern and constrain any cyber operations to which States or other parties to an armed conflict might resort. It is therefore crucial to ensure that, like any new technology, new cyber technologies that are, or could be developed or used for military purposes are capable of being used in a way that complies with existing IHL.

These days, cyber technology impacts most aspects of civilian life. The ICRC is particularly concerned, therefore, about the potentially devastating humanitarian consequences of cyber attacks on transportation systems, electricity networks and essential services such as water supply, health systems, dams or nuclear plants.

In December 2015, a cyber attack targeted electricity networks in Kyiv, Ukraine – a country involved in an armed conflict. Since then, Ukraine has suffered various other cyber attacks, including one in June 2017, which affected the Chernobyl nuclear-power plant. Criminal cyber attacks in 2017 (ransomware) have also highlighted the vulnerability of the medical sector.

Such attacks heighten concerns about the potential human cost of cyber operations and underline the importance of IHL's protective

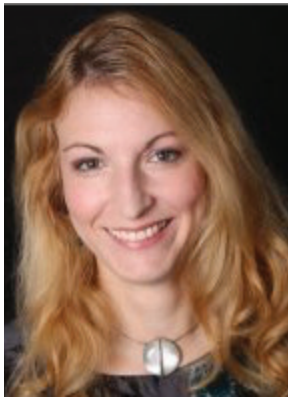
function as a legal "firewall" in cyber warfare to limit the effects of cyber operations in an armed conflict. According to the principle of distinction – one of the cornerstones of IHL – directly attacking civilian infrastructure is prohibited. IHL affords special protection to essential civilian infrastructure, such as water installations. The principles of proportionality and precaution afford additional protection to civilians, even when the target is a military objective. Already in peacetime, all feasible measures must be taken to protect the civilian population from the effect of hostilities. These include segregating military and civilian cyber infrastructure and networks, taking measures to guard against malicious software and making arrangements to ensure vital computer systems can be quickly restored following a cyber attack.

However, the specific characteristics of cyber warfare also raise challenges in terms of the application of IHL. Firstly, the anonymity of cyberspace makes it difficult to identify the perpetrators of cyber attacks. Furthermore, some focus only on the physical damage when assessing the legality of a cyber operation. In the ICRC's view, such a restrictive understanding of the notion of attack as something that causes only physical damage ignores the harmful effects that can be caused by rendering something dysfunctional without physically damaging it. This would make such understanding incompatible with the aim of IHL to ensure protection of civilians and civilian objects against the effects of hostilities. If the supply of electricity to the civilian population is disrupted, and if essential infrastructure such as medical services is affected as a result and patients die in intensive-care units, it is irrelevant whether the disruption to the electrical network was caused by a graphite bomb or a cyber operation. While the interconnectivity of cyberspace makes distinguishing between military and civilian objects more challenging, in most cases knock-on effects are foreseeable and must therefore be taken into account when planning or deciding upon a cyber operation.

Today, cyberspace is an integral part of daily life in most parts of the world. It brings enormous benefits but also poses inherent risks

and threats. We must all adapt to this new reality, and the ICRC, for its part, is constantly exploring the opportunities that cyberspace offers while being fully aware of the challenges and risks digitalization entails. The ICRC continues also to remind all parties of the importance of applying IHL in armed conflict to protect civilians from the effects of hostilities, whether they are cyber or kinetic in nature.

The Evolution of International Collaboration and Law Related to Cyberspace and Security



Kaja Ciglic, Director Cybersecurity Policy and Strategy

More than 30 governments have acknowledged that they have offensive cyber capabilities. However, unlike with conventional weapons, cyber arsenals are clandestine and intangible. Their source is difficult to track and identify. It is therefore likely that the real number is not only much higher, but will grow in the coming months and years. Moreover, because of this ambiguity, governments are more willing to deploy these weapons – testing capabilities with strikes, while tuning their strategies behind closed doors.

The cyber arms race is clearly under way.

However, the risk and dangers of cyber weapons are not well understood. These two issues together – the clandestine nature and the unpredictability of offensive online activity are creating vulnerabilities at a scale and speed that we haven't seen before. How can we manage the resulting risk, risk that can manifest itself both online and offline?

International Law Applies to Cyberspace

Microsoft believes that existing international law applies to cyberspace. This should hardly be a surprise. Online activities involve real people using tangible objects that have long been subject to various legal frameworks. However, it took governments a little longer to come to this conclusion. The United Nations almost two decades ago set up a working body to ensure agreement is reached on how to handle the then relative new field of information technology (IT), and in particular the increasingly difficult question of cybersecurity. It took a while, but in 2015 the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) confirmed that international law applies to cyberspace . The consensus report was unanimously adopted by the 20 countries that participated in the process, including the USA, China, Russia, France, and the United Kingdom. This position has been subsequently reaffirmed in several statements by individual governments, and indeed by the Group of 7 (G7) in early April of this year .

Today, therefore, the only way to ensure that the behavior of states in cyberspace is subject to certain rules and norms is through the recognition of international law.

Significantly, this stance is echoed in bilateral cybersecurity deals between what I call “cyber superpowers”. From the Sino-Russian , US-China , US-India and Sino-Anglo cybersecurity agreements to this year’s China-Australia cybersecurity cooperation agreement , there are many and varied references to the UN GGE and expressions of support for cybersecurity norms. Regional groups have similarly acknowledged the applicability of international law to cyberspace, including the ASEAN Regional Forum and the Organization of American States . Bilateral and regional agreements are important steps, but they do not address the need for a strategic international cybersecurity framework.

Today, therefore, the only way to

ensure that the behavior of states in cyberspace is subject to certain rules and norms is through the recognition of international law. The challenge, from our perspective, is not about the applicability of international law but its sufficiency and implementation during times of peace.

Commitment to International Law is Not Sufficient

Despite what appears to be almost unanimous agreement, it is proving difficult to travel from broad positions of support to concrete commitments. The UN GGE has been a key and constant part of this journey, the main highway, where other fora represented minor motorways. Now, we seem to have however hit a dead end.

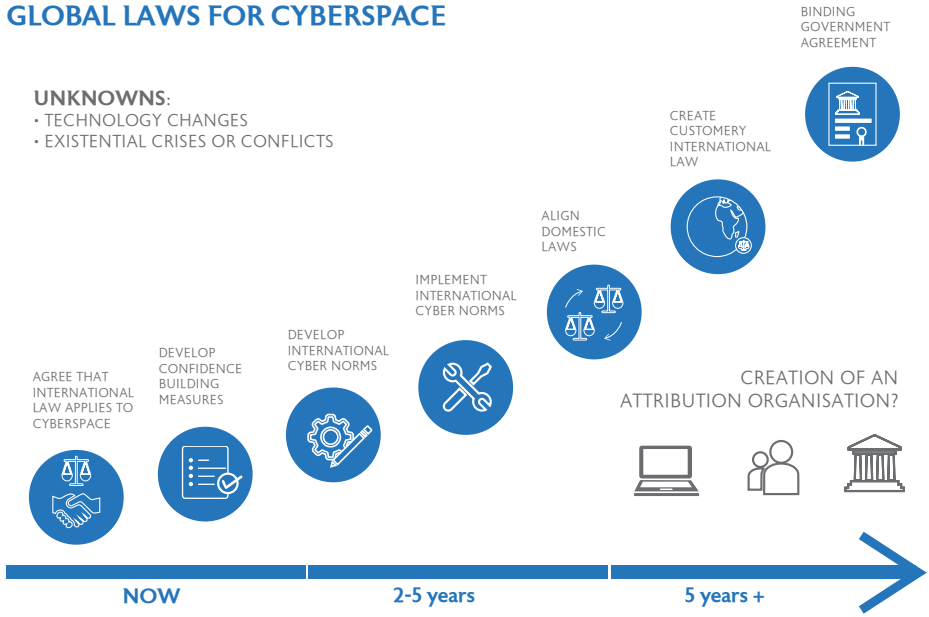
So where do we go from here? We do have the advantage of starting this complicated journey with an agreement on 11 cybersecurity norms from the 2015 UNGGE. We also have several proposals, including those put forward by Microsoft as part of the Digital Geneva Convention , and even partial agreements within narrower groups, such as the G7. But these are barely the first couple of steps on a long road.

To make significant progress, we have to unmask the fact that unfortunately there is little specificity in the agreements reached so far. This situation allows states to continue to act in violation of established norms, without the international community having any recourse to respond. For example, international law prohibits the use of force by states except in self-defense in response to an armed attack and the UNGGE norms call for states to refrain from international malicious activity. The questions are how these statements should apply to cyberspace, how concepts such as malicious activity are defined. This is where the work so far falls short. To move forward, these gaps will need to be identified and addressed. The work of the Global Commission on Stability of Cyberspace around what constitutes core internet infrastructure could yield important results in this regard.

Moreover, the current list of norms does not fully address the core drivers of instability in cyberspace. A limited set of additional cybersecurity norms in areas where existing rules are either unclear or may fall

short in protecting civilians in cyberspace need to be developed. This could include norms which explicitly articulate protections for civilians, even if they are implicitly contained elsewhere in international law. The development of these norms should be informed not just by governments, but also by civil society and the private sector.

would lead to the development of customary international law. In this process, governments need not only adhere to the norms themselves, but hold other nation states accountable – whether through punitive actions, such as economic sanctions or words of condemnation. Even where there seems sufficient evidence, states often choose not to act, in an effort



Third in this process is the actual implementation of established norms, which – underpinned by the legal opinions of experts in this topic -

to not rock other relations. But that is seen by other governments as an example that such behavior is permissible.

Only then we reach the final step in this process - the development of a binding international agreement akin to a new or "Digital" Geneva Convention. Most experts agree that this final step is likely to take decades, something we have been very clear about when we launched our idea earlier this year.

Core Principles to Guide Progress Towards a Digital Geneva Convention

So what did we introduce back in February? We called on the world to acknowledge that we live in a world that is growing more insecure every day. We suddenly find ourselves living in a world where nothing seems off limits to nation-state attacks, online. There are increasing risks of governments attempting to exploit or even weaponize software to achieve national security objectives, and governmental investments in cyber offense are continuing to grow. Our proposed response was a Digital Geneva Convention, that would commit governments to adopt and implement norms that have been developed to protect civilians on the internet, without introducing restrictions on online content. Just as the world's governments came together in 1949 to adopt the Fourth Geneva Convention to protect civilians in times of war, a Digital Geneva Convention would protect citizens online in times of peace.

Moreover, we acknowledged that no single step by itself will be sufficient to address this problem. We encouraged the tech sector to step together to do more, given its unique role as the internet's first responders and commit ourselves to collective action that will make the internet a safer place, affirming a role as a neutral Digital Switzerland that assists customers everywhere and retains the world's trust. We also called for greater action in improving the current attribution efforts – a critical challenge in the online space.

However, as mentioned above, while the direction of travel might be clear, we still need to map out the route to get there because, as highlighted before, the main highway has been washed away. I believe that if we regroup as a wider community of politicians, diplomats, technologists and citizens we can find our way to the next step. Not only are there numerous existing fora and groups that could be leveraged for this pur-

pose, there is increasing recognition that something needs to be done, and that it needs to be done before a cyberattack escalates beyond control. In other words, something needs to be done now.

However, we also need to be clear about how we are to make this journey. There are three main principles that must be recognized and adhered to for any effort to be successful:

1) We must have an open, multi-stakeholder process that represents governments, the tech sector, civil society groups and academia;
2) All parts of the world need to be represented and actively involved, from north and south, east and west and not just the "usual suspects";
3) The process cannot be locked away in committees that hide behind technical language, it must be open and transparent, so that everyone depending on cyberspace can see what is happening and can hold their governments, the tech sector and others to account.

If we ignore these basic principles and allow the process to fall back to closed, narrow groups then the world will stay where it currently is. We may make incremental, patchwork progress but it will be far slower and more limited than the rapid evolution of cyberspace and the attacks that take place within it.

Microsoft has made the case for a new commitment to the role of international law in cyberspace by calling for a Digital Geneva Convention. Our proposal represents the end of the journey I described here. The real question in our minds is therefore not how fast we can get to a new Convention, but how quickly we can make meaningful progress on the path outlined above. Waiting emboldens the status quo which means more attacks on civilians in cyberspace – with ever increasing consequences, effectively making cyberspace a lawless territory. We won't get there tomorrow. While this will be a journey through many iterations and staging posts, the destination of a stable and secure cyberspace will surely be worth the effort.

Finding New Rules for the Stability of Cyberspace

Marina Kaljurand, Chair, Global Commission on the Stability of Cyberspace

James Lewis, Commissioner, Global Commission on the Stability of Cyberspace

In a prescient speech at the 2011 Munich Security Conference, the UK's then-Foreign Secretary William Hague called for a collective response to the "dark side" of cyberspace. Hague wanted a "comprehensive, structured dialogue to begin to build consensus among like-minded countries to lay the basis for agreement on a set of standards on how countries should act in cyberspace." Hague identified seven, principles to guide work on norms and pledged to host an international conference. The Global Conference on Cyberspace to be held in Delhi, is the fifth of the series of international conferences that Hague began.

With one exception - the 2015 Conference in Den Haag - these previous conferences have fallen far short of the original expectations. They strayed from Hague's original idea of bringing like-minded countries together to give norms "real political and diplomatic weight." The confer-

ence organizers. The agendas tended to plow old ground, taking a "big tent" approach that encompassed a range of issues related in some way to cyberspace. Political timidity guided these earlier Conferences.

The Global Conferences took place against the backdrop of the work of the UN's Group of Government Experts (GGE). Unlike most GGEs, where academic experts explore a topic, these "Cyber GGEs" were in fact proxy negotiations, with countries sending diplomats rather than academics. There have been five GGEs. The first in 2004 failed, largely because of American intransigence. The last, in 2017 also failed, this time because of deep disputes over international law. But the three GGEs in between 2004 and 2017 succeeded in reaching consensus on norms for responsible state behavior in cyberspace.

All three GGEs were difficult negotiations. The 2010 GGE Report laid out the international negotiating agenda: cooperation among states on norms, CBMS, and capacity building. The 2013 GGE Report reshaped the political landscape of cyberspace with its conclusions that internal law, sovereignty, and the UN Charter applied in cyberspace. This anchored discussion firmly in the context of existing international relations. Building on this, the 2015 Report laid out a sequence of norms to guide state behavior: its report was endorsed by the members of the UN General Assembly. The 2013 and 2015 GGEs provide recommendations on norms that can provide the basis for international cooperation on responsible state behavior.

Rumours of the GGE's demise have been greatly exaggerated, but whether the failure to reach consensus in 2017 is only a pause in negotiation or whether the GGE process will be replaced by something else remains an open question. To be fair, the leading cyber powers - those who have the capabilities to exercise power in cyberspace - are not ready for agreement. Absent some truly pressing crisis, progress towards the

There are many contending agendas in cyberspace and powerful voices to advocate them.

goals Hague laid out will continue to be desultory.

One development that complicates defining the next step is that cybersecurity has gone from a specialized issue to one that touches many social and economic activities. All the GGE's acted under the auspices the UN's First Committee, which is responsible for disarmament and international security, but now a broad range of governmental and non-government bodies are attracted to the idea of developing norms. There is much room for many groups to work, as cybersecurity covers a broad range of issues, but the core issue of international security will remain closely held by states. Similarly, norms that do not win the acceptance of powerful states, such as the member of the five permanent members of the UN Security Council or the G-20, will not have useful effect. This is a hard truth from international politics, but this explains why the unfocused efforts of the Global Conferences before Den Haag made little progress.

The 2015 GCCS held in the Netherlands was an exception because it created formal structures on capacity building, information sharing, and a high-level Commission to consider how best to make cyberspace more stable and secure. These ongoing efforts are valuable, and the Global Commission on the Stability of Cyberspace (GCSC) most directly addresses the challenges of building stability in cyberspace.

The Commission has a challenge task and it faces some of the problems that afflict the GCCS series. The Commission's twenty-seven members, drawn from industry, technical and civil society have varied expertise and nationalities. There are many different negotiating cultures in the group. Internet engineers want precise technical definitions; business people wants detailed contracts with subparagraphs for all contingencies. Diplomats know the value of ambiguity in getting states to actually agree - details can be worked out once there is political agreement, not before. But all agree on the seminal idea behind the GCSC, that identifying norms for state and private sector behavior can increase stability and security.

There are many contending agendas in cyberspace and powerful voices to advocate them. The Commission is

another voice and it faces significant but surmountable obstacles. The first is finding the balance between the role of the public and private sectors. The gravitational pull of the multistakeholder model that has guided internet governance is powerful and many advocate using it to define and implement cybersecurity norms. The second is deciding whether more norms are needed or the existing international law and treaties and the GGE Reports are enough. The temptation to propose additional norms is also powerful. The third is how to scope its work and whether to focus on international security or to bring in other issues.

In the near term, the GCSC has considered proposing a norm to protect the public core of the internet, a proposal advanced at the 2017 GGE. The draft language being discussed is:

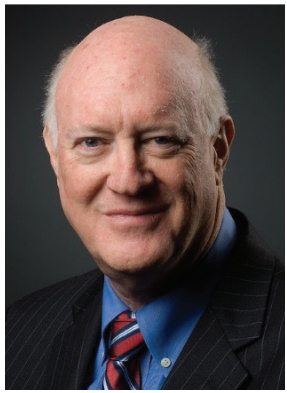
States should not conduct or allow ICT activity within their territories that would affect the general availability of the core naming and forwarding functions of the internet.

While this language did not meet with universal agreement among GGE participant nations, the GCSC has the freedom to recommend it or an amended version of it for renewed consideration by international bodies like the G-20 or others.

In the long term, the GCSC could usefully consider how norms can be made more effective, the role of attribution in this, and whether a normative structure requires some kind of a formal, institutional framework or a convention. In considering all these issues the GSCS can help redefine the relationship of the multistakeholder model to international security.

The GCSC offers the best the opportunity to fulfil Hague's wish for a comprehensive, structured dialogue to build consensus and lay the basis for agreement on norms. It can only make recommendations for others to act upon, but it has a unique status and with that, a unique opportunity to identify the path forward for stability in cyberspace.

Cyberspace Challenges: Past and Future



Stephen D. Crocker, Former Chairman of the Board, ICANN

Next year, computer networks will be 50 years old. In August 1968, I was lucky to be part of a small group of researchers and students in sunny California who started trying to connect computers located in different physical locations.

By the end of 1969, there was one rudimentary network linking four computers at four research centres: University of California, Los Angeles (where I was a student); Stanford Research Institute; University of California, Santa Barbara; and University of Utah in Salt Lake City. I offered to organise our early notes. What was supposed to be a simple chore caused me considerable trepidation.

We wanted to encourage others to chime in, but I worried we might sound as though we were making official decisions or asserting authority. To make sure that I did not miss any inputs from peers or senior professors, I wrote a note which I labelled "Request for Comments 1" (RFC 1),

leaving many questions unanswered. Though RFC 1 would soon become obsolete, the RFCs themselves took root and flourished. They became—and still are—the formal method of publishing internet protocol standards, and today, there are more than 8,000 [RFCs], all readily available online.

Along with the expansion comes new challenges and opportunities. Our challenges 50 years ago were very different from the challenges we face today.

Over the past 20 years, the internet has delivered the power of connectivity that was unimaginable 50 years ago. More than 3.7 billion people are connected through the network of networks we call the "internet," with more than $2.3 trillion changing hands through e-commerce. Access to the top-level domain of the internet is now available in 20 non-Latin scripts, something I am personally very pleased about. Expansion of the network is rapidly continuing across different operating systems and devices, most notably in the mobile sphere.

Along with the expansion comes new challenges and opportunities. Our challenges 50 years ago were very different from the challenges we face today. Where once we grappled with the initial challenges of connecting computers of diverse manufacture, we now work with a multitude of applications, communities and languages. And, of course, we also have to contend with serious security challenges.

Thankfully, sustainable governance structures now exist to facilitate the spread of networks across the globe. There are forums available for those who wish to participate and contribute in building the "internet of the future," whether in the technical space or the policy space, with the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Engineering Task Force as just two examples. We need to continue to work together with each other to address these challenges.

The Fifth Global Conference on Cyberspace (GCCS), taking place in New Delhi, offers the world an

important opportunity to do just that. The key themes for this conference—cyber growth, cyber inclusion, cyber security and cyber diplomacy—are where the discussions need to be, where we need to continue to develop solutions, for the benefit of humanity.

Since the conference takes place in India, I am reminded of my first visit to Bangalore in 1994. I was invited to give a talk at the Indian Institute of Science, and as part of the visit, I was introduced to a student who had built a fairly complex software system. Impressed, I asked where he had learned to do so much. He simply said, "I downloaded the RFCs and read them." This is the power of the internet. We need to continue to do more.

In closing, I wish the hosts—the Government of India, and the participants at the GCCS conference—every success. I look forward to reading the takeaways from this meeting.

20 ROUSE AVENUE
NEW DELHI 110 002
INDIA

P +91 11 4352 0020
F +91 11 4352 0021