




**Cyber Security, Cultural Security and the Cyber Gap:  
Lessons from Middle Eastern Policy Makers  
Cultural Security:  
Concepts and Applications**

**Prof. Dr. Brian Brivati**  
Academic Director, PGI Cyber Academy

**Brian.Brivati@gmail.com**

**Received:** 16 August 2017  
**Accepted:** 21 November 2017

Turnitin - passed research



## Abstract

States face ever increasing ethical, legal and rights challenges thrown up by cyber security issues both in terms of national security, the protection of cultural norms and in terms of privacy and commercial activity. These challenges interface with greater demands for online human rights across a broad spectrum from the defence of IP to the protection of identity and the limits of surveillance. There are significant variations in the level and quality of policy frameworks that respond to increasing economic reliance on internet based activity. The link between the effective operation of a national cyber security plan and the promotion and defence of online human rights in terms of national, regional or global human rights norms in what will be an ever more complex and disputed area, requires a platform for training and sharing of best practice. There have been a range of initiatives from the international donor community to engage with individual countries and to set global standards. There has been little specific and sustained focus on the interface between security and rights because different departments tend to focus on these issues. In turn, different states have widely differing conceptions of freedom of expression and cultural norms that should be allowed.

This paper builds on a three year multi-country project that has established a network of cyber policy experts across the Middle East. It explores the need to manage the trade-off between public expectations of privacy, cultural difference and the need for state surveillance in cyber space. It presents the preliminary conclusions of a group of policy makers who took part in a multi-stage Fellowship programme. This group pulled back from considering some key issues, accepted profound differences of approach on other issues and devised an agenda of collaboration in spaces that they felt progress could be made on. The paper concludes on the needs to more Fellowship style network policy making and presents a broader theory of change model for developing policy responses to the challenges of cyber-crime.

**Keywords:** *cyber security, cultural security, Middle East, Cybercrime, global human rights*



## Context

The internet is the most powerful engine for global economic growth, enterprise, innovation and productivity we have seen for the last one hundred years. It has reduced distance to such an extent that it has laid the foundations for the development of a single global community. At the same time as an engine for freedom of expression it has created a myriad of global communities of shared interests and beliefs. It allows for the connectivity of citizens enabling unparalleled political activism. It is a utopia of instant communication. It is better than any science fiction.

The challenge we now face is how to make the internet safe without resorting to the Leviathan<sup>(1)</sup> of a Hobbesian state that sets out to control everything. It may be that we are already<sup>(2)</sup> too late. Another Leviathan, organised crime, inhabits large parts of the dark net already. Criminals abhor a vacuum. When they realised that by shuffling IP addresses they could not be traced they filled the dark net. Ironically it was the CIA that created the ability to hide so that their agents could not be traced on the internet. Now they have to deal with a vast dark cyber space in which anything can be bought and sold.

As the open and the dark net have grown so they have become home to both the best and the worst of humanity. For every action that furthers freedom on the Internet there seems to be a new use that exploits or degrades human beings. It also gives states powers of surveillance that even Big Brother could only have dreamed of. As states have tried to assert control, so this in turn has pushed the misguided, the naïve and the perverted into the dark net. What they find there is a place outside the law, outside the reach of the state. They will enter the state of nature.

The French philosopher Jean-Jacques Rousseau postulated that in the state of nature the best of humanity would shine through. The English philosopher, Thomas Hobbes disagreed. He postulated that in the state of nature the worst of humanity would flourish. The internet has created a state of nature and the jury is out as to which philosopher will be proved right.



Historically governments through law and regulation, civil society institutions like schools and churches, mosques and law enforcement agencies have existed to protect citizens organised into a state from a state of nature in which human creativity and depravity go unchecked. For Rousseau these were chains that entrapped people who would otherwise be free. For Hobbes there were necessary barriers that saved humanity from itself. These barriers of protection and these rule books for enabling have been rendered largely redundant. At the time of writing it is Thomas Hobbes who is ahead on points in cyberspace and in what humanity does with freedom.

Cyberspace can still reach its full potential and continue to transform the world for the better. But states must make cyberspace safe enough to maintain public and commercial users' confidence in it. They must also allow it to remain open and build legitimacy into the regulation of its operations. They must allow for the protection of values and the diversity of cultures that promotes cosmopolitanism. While they must combat serious and organised criminals who use the internet to organise, equip, and perpetrate crimes such as fraud and child exploitation, they must also defend and protect the rights of citizens to use, organise and communicate positions critical of their own governments. States need to defend themselves, their critical infrastructure and their people from profound external threats. Extremely powerful and intrusive capabilities – technologies, legal powers and cyber skills – are available to help them do this. The use of these powers entails ethical and legal challenges. National security, human rights, technological innovation and commercial interests form the arena in which the future of the internet will be shaped. At the moment the shape of that future is uncertain<sup>(3)</sup>.

At the interface between state action and internet use sits the need to balance reasonable public and corporate expectations of privacy and safety and security. States use capabilities in technology, intelligence and surveillance to carry out their protective duties. These activities must be enabled and regulated by national, regional and ultimately global legislation. There is, however, no easy, generic solution. No one country's model will work precisely for another. In addition, while each state must take a route that works for them,

states cannot act alone. Cyber space is borderless, its criminals international. National responses are more effective with support from regional and international partners, underpinned by common principles and standards.

To understand these principles and standards, the debate must be technically well informed. This is the heart of the matter. It is the reason that what has been unleashed on the world is out of control. Many recent examples have shown that those responsible for law enforcement have no idea what is going to happen next. That aggressive states are attacking their rivals and their neighbours in a multiplicity of ways that sometimes do not emerge until long after the event. That legislators, because they do not understand the technology have little idea what they are making legal or illegal in the measures that they are passing.

Jurisprudence over an area that expands in ways that the drafters of law do not understand is not a new phenomenon. The invention of cars required the imposition of speed limits. It is the expedient systemic nature of innovation in information technology that creates a problem of new proportions. It is like inventing something equivalent to a motor car every few days over several years and trying to legislate to control their impact on society, culture, geography and safety. But not only does the law not map onto the new worlds that are being creating.

Criminals have always and will always find new ways to break the law and steal what they want. But now eighty per cent of crime committed in the UK, for example, is cybercrime (that which can only happen because the internet exists) or cyber enabled crime (crime that is made easier by the presence of the internet). That means that there are now entirely new categories of crime being committed. Entirely new crime scenes being created often not in the same location as the criminal. These crimes are taking place in a context that officers openly admit they do not fully understand and do not have the skills or the tools to properly investigate.

If the state in the shape of its legislators and its law enforcers is out of its depth then so too are the defenders of internet freedom. Arguments for Freedom of Expression as an absolute right stood

up well within a world in which information could be mapped and identified clearly, when civil society was strong and when access to depravity was limited by the physical challenges of distribution. There are no longer barriers to access afforded by controls that allowed for universalism. Moreover, the political freedoms afforded by the flow of information on the internet can be used to recruit extremists of all kinds, distribute hate literature, incite violence against individuals and communities and ultimately through cyber warfare be the means of delivering attacks on critical infrastructure anywhere in the world, at any time.

To navigate our way through the contemporary state of nature that we find ourselves in, the experts in the science of security and technology need to be involved in the discussion alongside experts from law enforcement and intelligence agencies, alongside human rights lawyers and advocates. But here we come up against The Two Cultures<sup>(4)</sup>.

C.P. Snow, an English writer and a scientist, laid out the divide between Science and the Arts in a famous Rede lecture delivered in the 1950s:

“The non-scientists have a rooted impression that the scientists are shallowly optimistic, unaware of man's condition. On the other hand, the scientists believe that the literary intellectuals are totally lacking in foresight, peculiarly unconcerned with their brother men, in a deep sense anti-intellectual, anxious to restrict both art and thought to the existential moment. And so on. Anyone with a mild talent for invective could produce plenty of this kind of subterranean back-chat. On each side there is some of it which is not entirely baseless. It is all destructive. Much of it rests on misinterpretations which are dangerous.”

In the case of the modern internet we face a three culture problem of a kind that Snow would have recognised, though there are important differences. We all use the technology. In that sense the cultural position of technology has alternated significantly since

Snow's day - he was writing in 1959. But only the technologists and scientists understand the technology. The Human Rights industry is not technically expert but they are predominately lawyers and so they see the world through a very particular prism. The police and the intelligence services might come from arts, social science or humanities background, but they now see the world from a law enforcement perspective. If not three separate cultures, we are certainly talking about three mutually uncomprehending dialects.

This situation needs to change and quickly. There needs to be a forum through which translators can work to enable a dialogue. Each side has valid and important things to say about this debate. A rights based approach is needed in a democracy but it must be realistic. States will not abandon the use of this technology to defend the security of their citizens so freedom of expression advocates need to engage in debate and dialogue with governmental cyber policy makers. In turn, law enforcement must engage with lawyers to understand and agree the limits of what is acceptable rather than what is merely technologically feasible. The security scientists and technologists must hold the ring. They alone can provide the tools to monitor and evaluate what is being done and how it is being done. But they can also keep both of the other two groups informed of the pace, extent and capability of what is happening in cyber space and what it means for the lives of citizens. There needs to be an open and frank dialogue between human rights activists, the University experts in security science and the private sector cyber security industry and government officials at the front line of fighting cybercrime. The challenge is to create the forum in which this dialogue can take place.

What happens if the three cultures do not come to together to tackle these issues? If we are to avoid the creation of a series of internet silos, in which states create walls around their citizens own use of the internet, then we must develop regional legislative and cooperative structures.

Cybercrime grows in parallel to the growth of the internet. As usage increases, crime via the internet will also increase. There will soon be four billion people online. In 2014 estimates of the cost of Cyber-

crime varied from \$500billion to \$1trillion: all the experts agreed that it was increasing and that 75% of all crime was technology enabled in some way. It is a high profit, low risk crime. Getting away with it is easy as the criminal is not linked to the crime scene. A fundamental principle of policing has been removed. As Troels Oerting, the Head of the European Cybercrime centre has recently put it, "We are fighting 21st Century crime with 19th Century tools". While banks and large companies might be able to protect themselves, individuals and Small and Medium Enterprises (SMEs) are extremely vulnerable, and citizens are very bad at their own cyber security.

Cybercrime presents investigative, ethical and legal challenges for law enforcement officers and telecommunications policy makers in government that need to be recognised by freedom of expression advocates. States need to understand the nature of these crimes and the role of states, organised crime and individual criminals in their perpetration. They need to know how technology is developing to enable crime, its prevention and intelligence operations. But they also need to understand legal constraints on the actions of intelligence agencies and law enforcement in circumstances where law is often running behind technology. To ensure prosecutions are successful, they need to allow evidence to be assembled in ways that will make it admissible and identify the jurisdiction within which the crime can be prosecuted. They must also ensure that it is real criminal activity that they are targeting and not legitimate political or cultural activity.

A further challenge is presented by the international dimensions of the problem. The internet eliminates borders and the territoriality of the rule of law. Cybercriminals therefore operate without borders. Those who seek to prevent criminal activity on the internet tend to be hampered by boundaries between jurisdictions, competition between agencies and differing standards, terminologies and penalties. In the absence of robust and enforced legal frameworks, networks within countries' borders can be used to store and transport information and conduct operations that are illegal elsewhere. This reality raises many questions for human rights advocates defending the universalism of freedom of expression in the UK.

A yet further challenge is presented by the need to manage the balance between public and corporate expectations of privacy, the



rights of the accused and the need for state and law enforcement surveillance in cyber space. The programmes and processes that are used to gather intelligence to prevent cybercrime, combat hostile foreign activity and keep citizens safe from criminal and external threats give the state extremely powerful and intrusive surveillance capability. States must use this capability to fulfil their responsibility to protect, prevent crime and secure convictions while meeting the reasonable expectations of everyone who is using cyber space that they will be able to go about their business safely, freely and in private. States must also seek ways to capture, investigate and punish perpetrators while also respecting the legal rights of the accused.

The substantial and layered ethical dilemmas posed by the use of the capability developed to protect and investigate in this field are made even more acute by the absence of a single, internationally agreed legal framework. The construction of international law is struggling to keep up with the speed of technological advancement. As international and national laws and best practice are still developing in this area, many policy makers believe there is no single right answer or generic template which can be applied. Instead, a balance must be struck appropriate to the threat, national intelligence and law enforcement systems and processes as well as prevailing cultural and international norms. This balance must then be enabled and regulated through the development of nationally appropriate legislation which is understood, enforced and promoted by those who are conducting operations and developing national offensive, investigative and defensive capability. In turn experts in the technology itself must be central to the process of law making so that the regulations are actually keeping pace with the capabilities.

Many campaigners reject these claims, holding to the notion of the universal applicability of freedom of expression and other rights. The role of a Forum is in part to explore what common ground can be found between these two positions. The rapid development of such appropriate frameworks will be enabled by sharing information between the policy makers who are trying to frame law and policy in this rapidly changing field, technologists and scientists who understand that nature of the change taking place and rights advocates who are campaigning for an Open Internet.



When the Green Paper was drafted the Fellows meet together to build on their work and then completed a White Paper for the region and individual country White Papers. The production of the agreed regional White Paper, which is on-going, will establish a model which is available to all countries in the region and – if they chose to adopt it – to which they can move at their own pace and in their own ways. It also gives a regional framework of reference for future discussion. The influence of the individual country White Papers and the debate and discussion which creates them will place an ethical approach at the centre of the cyber regulatory agenda.

The project is split into different country zones to reflect different regulatory frameworks and political contexts in which the network will operate<sup>(5)</sup>. While countries in the region may not all implement regional and global rights frameworks and the impact in the different zones will vary, the existence of the White Paper will ensure that the debate in each country with respect to the principles and guidelines for internet governance will be better informed.

The Fellowship is also a network which can form the basis for mutual legal assistance within and between the states involved.

The Green Paper discussion generated the following core areas of debate, which require further work in the White Paper stage and which address various aspects of the context described above. This is based on a two day meeting in London between policy makers and law enforcement officials from ten countries across the Middle East. The discussions were facilitated by UK experts.

Core issues that emerged:

- **Social Media and Censorship**
- **Law and Law Enforcement**
- **Ethics**
- **The Human Factor**

The main points that emerged from these discussions are summarised below and possible solutions to be explored at subsequent stages in the process are outlined:

### **Social Media and Censorship**

There is debate surrounding whether censorship should be the responsibility of the state or the companies controlling the content. Social media services are unwilling to transform their role from platform to editor, partly in the attempt to meet the interests of their founding ideology and shareholders. Companies may also struggle to ensure consistency in the editing of their content if they adopt a purely reactionary response to inappropriate content. However the different dimensions of the need for censorship on social media are increasingly compelling.

### **Solutions Discussed**

- Train authorized flaggers who work with social media to inform them of potential infringements that may be removed under the content agreements between social media providers and the client.
- Investors and advertisers, reluctant to be associated with providers hosting inappropriate content, may provide background pressure and should be encouraged to do so.
- Increase the presence of positive content through “teaming” and civil society groups, mosques, and moderate political parties to flood social media and swamp the extreme content.
- Combating Content: Simply blocking an account generally fails to prevent repeated misuse, merely forcing the individual to create new accounts or move to new social media platforms so addressing radicalisation at source or disrupting the payment process for the purchase of pornography is being explored.
- Removing content should also occur alongside other methods, including using geo-mapping to identify and target the ecosystem of the repeated attacks’ origin.
- Technical improvements on websites such as the algorithms used to detect child pornography.

## Law/Law Enforcement

Cross Border Attacks: Cyber-attacks are often cross-border. This inhibits a state's ability to prosecute and combat attacks not only because of the reliance on the cooperation of another state's law enforcement agency but also because that cyber activity may not be illegal in that state's jurisdiction.

### Discussion Points

- The lack of resources and competing priorities prevent law enforcement agencies from responding to prosecution requests quickly. Providing feedback on how response connects to their remit might improve the service.
- Laws are unable to keep up with the technological advances used by cyber criminals. Private companies thus often become the first line of defence in responding to attacks. Even in the UK Civil Contingencies Act there was no provision for the role of police in a cyber-attack until the Investigatory Powers Act was passed in 2016<sup>(6)</sup>.
- During the investigation and prosecution process difficulties can arise from the number of different parties involved, including law enforcement, security and government departments.
- The potential need for new legislation to cover specific areas, such as big data and cloud forensics was demonstrated by the UK Investigatory Powers Act in 2016. Many activists opposed it but most elements of law enforcement welcomed it.
- There is a real need to bridge the gap between the public and private sector in exchange of information about cyber threats and attacks.

## Potential Solutions

- Interpol: potentially good candidate for dealing with cross border crimes but competing demands and priorities often lead to poor response times.
- Bi-lateral/multi-lateral agreements: Success is dependent on the nature of the agreement and may still suffer from differences in jurisdictions and law enforcement priorities.
- Formation of a regional group to encourage sharing of information and cooperation in the pursuit of cyber-crime is essential and could mirror the work of EUROPOL.
- Encourage development of domestic university programmes, businesses and industries in cyber technologies and methods to help bridge the gap in supply and demand in the cyber field.
- If cyber-crime were regarded not as an entirely new crime, but rather as conventional crime with a cyber-component, this might offer a means of combating the rate of developing of cyber-attack advances.
- Laws, like the UK Computer Misuse Act, should be flexible and general enough so that new attacks can be included within its existing clauses rather than require constant amendments or new laws.

## Ethics: Discussion Points

- The complex dynamics of cyber-crime raises a number of key issues including:
  - accountability and boundaries
  - Responsibility for mitigating risk
  - Managing consequences of an attack
  - Privacy and security.

There is a need to ensure that individuals understand the ethical demands of decision making in responding to cyber-attack crises. Individuals are much more sensitive to state sector intrusions into privacy than private sector intrusions, despite this being a major ethical issue.

There remains a general lack of awareness about the extent of the information companies are able to gather from applications and other cyber information.

### Potential Solutions

- Creation of a Digital Ethics Panel based on consultation with different fields, such as security, intelligence, policing, law enforcement, academia and pressure groups, to explore ways of regulating and framing ethical decisions. This offers the potential to fill those areas where the law has failed to adapt to the changing threat.
- Use of simulated cyber-attacks provides a company/country with a procedure for facing the threat and prepares individuals for the ethical decisions they must make in response to it.
- Regulation that supports informational privacy, allowing individuals to specify that his/her data only be used for a specific set of purposes.

### The Human Factor: Discussion Points

Surveys of government employees demonstrates that, despite high levels of confidence in working with computers, employees can fail to recognize the importance of the information they have and make rudimentary security mistakes. It is often the Human Factor that allows the security breach to take place.

### Potential Solutions

- Banning one form of insecure data transportation, such as a flash drive, does not prevent exposure to risk. However, employees often turn to another equally insecure method to transfer data.
- Creation of a “cyber aware” ethos in the company and basic cyber awareness training may be a means of combating this.

In the final session of this first meeting of the Fellowship, the team discussed and agreed on a set of working principles and practices that would inform the on-going development of the regional response.

## Conclusions of the Initial workshop of the Cyber Fellowship

### Statement of Principles and Working Practices

#### Principles:

- The Fellowship will only work on the most difficult problems that need to be dealt with by a cross country, cross-disciplinary team.
- The Fellowship is agreed on the importance of sharing information as partners and that political issues should be absent from its work and the formulation of this paper.
- It recognizes that whilst alliances and relationships may change there are shared areas in which cooperation to increase each country's cyber capacity overrides political issues.

#### Working Practices:

- Each working group of the Fellowship has undertaken to complete a section of the Green Paper.
- The UK team are a resource that can be tapped into to support this work. It is up to each working group to decide on the working practices and division of labour that will allow them to meet the deadlines that were agreed at the final session of the Fellowship.
- The drafts of each working group will be circulated to the whole Fellowship for discussion and debate.
- Our working model will be one of consensus with minority reports. The consensus model is one in which the conclusions and recommendations arrived at by the Fellowship will comprise only those things on which there is consent. That does mean that every detail and the style of writing is agreed upon. It does not mean that all the material in that specific section is agreed to by all the Fellows.



- In areas in which individuals or groups cannot agree to significant conclusions or recommendations, then they will submit a minority report. It is important to stress that minority reports are based on difference of substance across regions or between Fellows.
- The drop box folder is designed for storing material that is not confidential but useful for reference purposes for working group discussions. Fellows who are happy to can store drafts of Green Paper material in drop box otherwise each working group should decide on the sharing mechanism that they favour.

### Framing the Future Discussion

- Three key areas of cyber-crime emerged as potential for the focus of the paper: terrorism, inter-state attacks, and cyber-crime.
- Cyber-crime is most likely the area in which substantial progress can be made by the Fellowship.
- Terrorism is already comprehensively covered, and inter-state cyber-attacks are generally bilaterally focused on a particular target. However, cyber-crime targets any potential source of pecuniary advantage, regardless of borders or political machinations.
- States in the Middle East are currently poorly served by Interpol, and so developing more effective cooperation between fellowship countries may offer a means of more successfully combating such activities.
- The practical solutions developed by the Fellowship to combat cyber-crime will in many cases also be transferable to improve the fight against terrorism, extremism and inter-state attacks.

## Next Stages

The initial discussions summarised above are now to be developed. The idea is to build on and extend the existing PGI Cyber policy makers network by conveying the first standing conference on cyber security policy issues informed and influenced by UK experts and best practice in the region and support this with a series of specific policy based projects. The network identified key areas of risk that need addressing across the Middle East and key areas of best practice reflecting British and other international expertise that need to be developed. The delivery of these projects would enhance global cyber security by spreading across over ten Arab states, through the development of individual and joint projects, contemporary best practice. The hope is also that they will build sustainability into a network that can respond and adapt across the region to new challenges as they arise.

The Cyber Policy makers' network encompasses some fifty individuals across ten Arab countries. The next stage of the network is to develop and support a series of joint projects that have been proposed and developed at the White Paper stage of the programme. This will take these concepts through to be ready for delivery with support from regional donors in 2017-19. It will take the network from a peer to peer network of policy experts and develop it into a project-network which extends the peer to peer connectivity into the implementation of joint projects informed by the network participants and joint projects designed and delivered by the team.

The projects link international experts to policy makers and practitioners across the region and was developed through a combination of regional development meetings and expert lead webinars. Over the next calendar year the Fellowship will concentrate on the white paper stage projects, two of which will be ear marked for separate support, but all of which will link regional with UK experts in the peer to peer/ project delivery network. In 2018-2019, the Fellowship will seek support to extend and expand the network further across the region and deepen and extend the impact of the projects and policy initiatives generated.

The agenda for 2017-2018 is therefore shaped around taking forward the following projects which will be explored in greater depth in a series of ten webinars with UK experts:

## Trust

1) Learning from Precedent – What were the lessons that the UK learnt during the 6 or 7 years it took to develop IISP

- Develop a case study of international best practice and disseminate
- Develop a model of regional best practice and disseminate it
- Develop a methodology for Gap analysis between the two

2) Identifying and marking trusted organisations

- Develop guidelines for developing a 'safelist' of endorsed/accredited companies
- Design a model of existing best practice for trusted/preferred partners (e.g. Cyber Essentials?)

3) Design a model for forming a multi-sector committee which could formulate requirements and develop the community of trusted partners

## Critical National Infrastructure/Critical Information Infrastructure

Design and disseminate a road map for benchmarking critical national infrastructure with recommendations for implementation, to include

- Methodology for identifying formal national strategy to identify CNI
- Identify and study an international success stories and assess why certain aspects were/were not included
- Design a case study should be from outside the region, to be followed by one from inside (e.g. UAE or Qatar who have a mature understanding)

Following this, conduct Gap Analysis and Risk Assessments on other countries in the region to establish way forward to effectively identify CNI.

### Capacity Building

- Design a case study of the finance sector to use as a model for thinking about and engaging private industry
- Translate and disseminate UK materials for cyber security training in Schools
- Disseminate the model of the UK Cyber Security Challenge
- Develop a model of a Cyber Academy (i.e. a Fast Track) where individuals are given 16-20 weeks of upskilling training – this could be run by the public or private sector
- Develop a model of another public institution (comprising Government, private industry and NGOs) – rather like Academic Centres of Excellence – to cover Theory, Practical Experience and Training
- Study an established model which could be adapted by the Fellowship to identify courses that meet certain criteria and could be badged/certified within the region – e.g. GCHQ's Academic Centres of Excellence

These projects will be developed into concept notes and project proposals at two regional meetings and a series of expert lead webinars over the course of 2017-2018. Built into to these meetings and seminars will be strategy discussions for leveraging support from regional and other global sources to take projects through to implementation.



## Conclusions

To fight Cyber Crime, defend our cultures and our values, we need law enforcement tools that match the weapons of the criminals and the terrorists. But we must also defend our freedoms. To fight international crime we need law enforcement to be international, to be able to cross borders and jurisdictions as fast and as effectively as the criminals and the terrorists do. In both cybercrime and international terrorism we face a network of networks so we must build networks of experts who cross cultural divides to speak to each other and shape collective responses. The Cyber Policy makers Fellowship programme has been an attempt to build the kind of network that is needed in this space. But on its own it is not enough. It forms one part of a broader project to map policy responses that are needed in the current situation. By way of conclusion, the following slides show the mapping out of a broader set of initiatives and programmes that would build the capability needed to provide greater human security against the threat of Cybercrime.

### The Global Cyber Security Skills and Policy Gap

#### The Problem

- Global challenge of technology enabled crime increasing faster than response from government or private sector
- Global shortage of cyber security skills and knowledge in technology and security-related professions
- Global shortage of cyber security expertise in law enforcement and judiciary
- Cross cutting threat that encompasses national, human and economic security
- Transnational threat that requires national and international; solutions



Accountability from Pre



### Lessons from Precedent

- National solutions must feed into regional and global solutions but states will retain high levels of control
- Human Factors are as important as technology in meeting the challenge
- Solutions will only be derived from Public-Private partnerships
- Learning must be experiential because of the speed of change
- Any improvement in security and response makes everyone safer



### Challenges to be addressed

#### Skills and Knowledge shortage

- Specialist Cyber Security
- IT departments
- General Workforce
- Public Sector Employees
- Law Enforcement

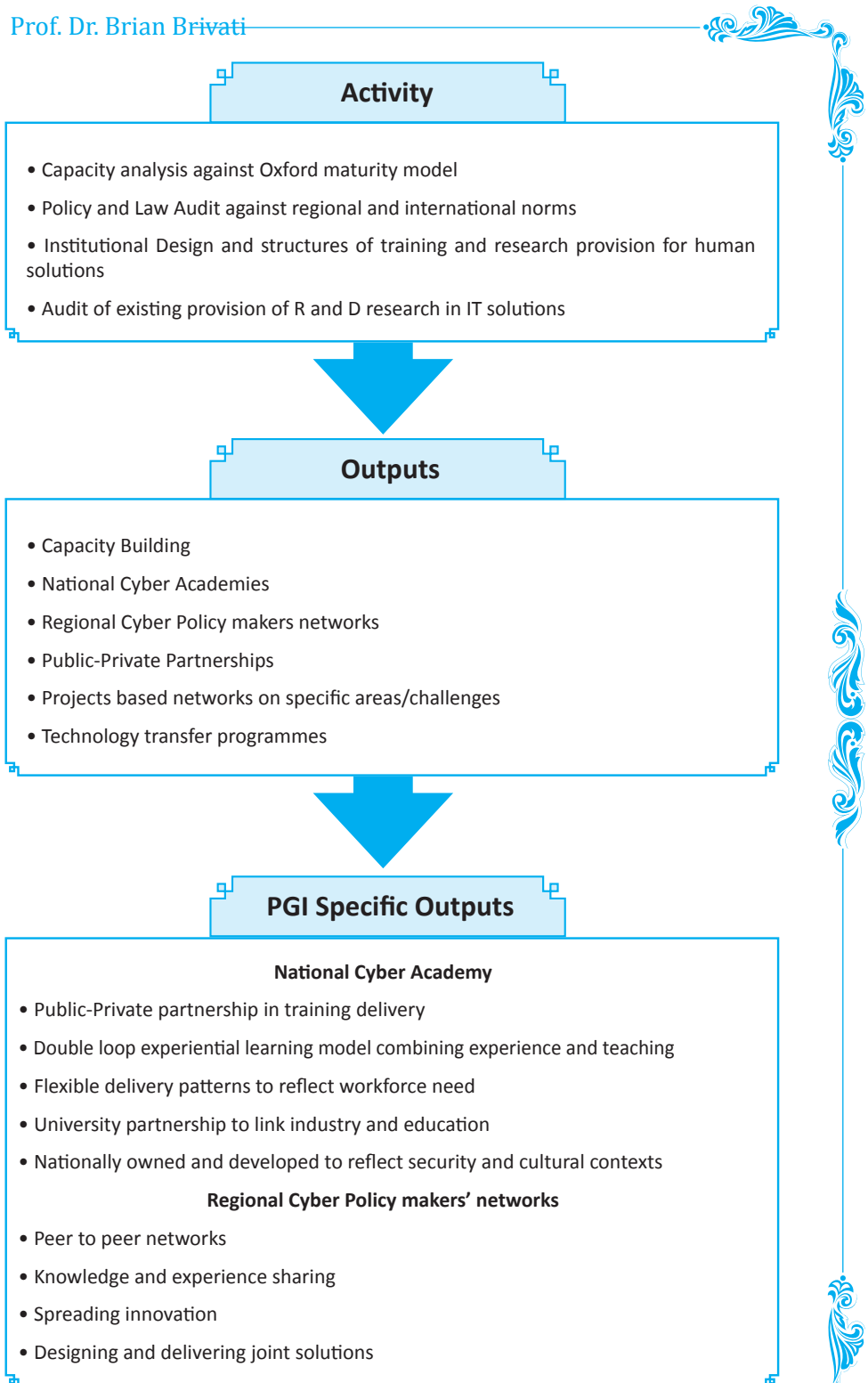
#### Policy and technology gaps

- Judicial Competences, Human Rights and Transnational jurisdictions
- Identity protection, System integrity and defence



### Inputs: Each country requirement different

- Support for Institutional Design
- Provision of Legal capacity building
- Funding of Technology transfer





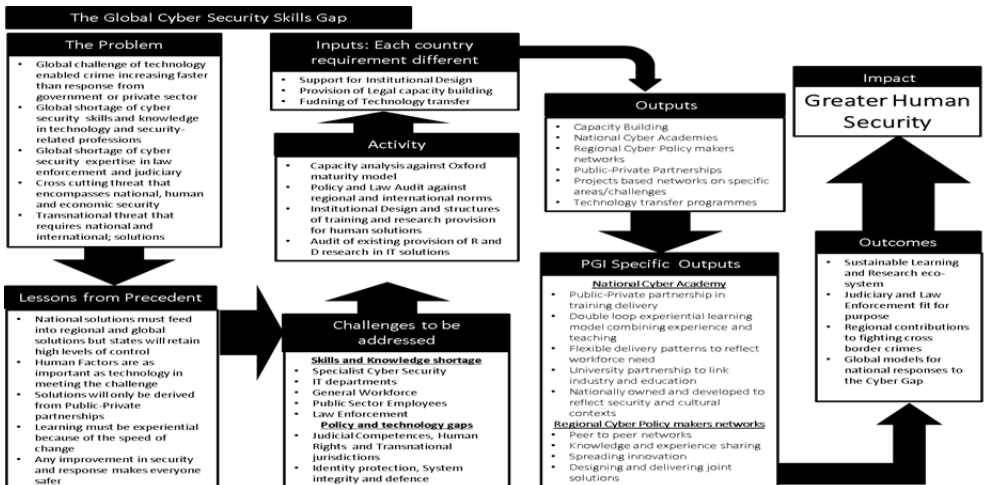
## Outcomes

- Sustainable Learning and Research eco-system
- Judiciary and Law Enforcement fit for purpose
- Regional contributions to fighting cross border crimes
- Global models for national responses to the Cyber Gap



## Impact

# Greater Human Security







## References

1. Thomas Hobbes, *Leviathan*, edited by Richard Tuck, Cambridge University Press, 1981
2. Evgeny Morozov, "The Net Delusion", Public Affairs, 2011
3. Clay Shirky, *Here Comes Everyone*, Penguin 2009
4. Charles Percy Snow, *The Two Cultures*, Cambridge University Press, 2001
5. Jean Jacques Rousseau, *Rousseau: The Basic Political Writings*, tr. Cress, Hackett, 1991
6. The Investigatory Powers Act legalised powers that the UK security services and police had been using for years after the investigatory powers tribunal, the only court that hears complaints against MI6, MI5 and GCHQ, ruled that they had been unlawfully collecting massive volumes of confidential personal data without proper oversight for 17 years. This brought their ability to combat Cybercrime within the legal framework of the UK

## Further Study

1. Cindy J Smith et al, *Routledge Handbook of International Criminology*, Routledge, 2011
2. Ngo Fawn and Raymond Paternoster, *Cybercrime Victimization: An Examination of Individual and Situational Level Factors*, *International Journal of Cyber Criminology*, Vol. 5, No. 1, January-July 2011
3. Richard Bressler et al, *New Global Cybercrime Calls for High Tech Cyber-Cops*, *Journal of Legal, Ethical and Regulatory Issues*, Vol. 19, No. 1, January 2016

