AIIA Policy Commentary

ICT4IR: International Relations in the Digital Age

Documents:

Commentaries:

Copyright © The Australian Institute of International Affairs 2011

ISSN 1838-5842

This publication may be distributed on the condition that it is attributed to the Australian Institute of International Affairs.

Use for educational purposes is not allowed without the prior written consent of the Australian Institute of International Affairs.

Any views or opinions expressed in this publication are not necessarily shared by the Australian Institute of International Affairs or any of its members or affiliates.

Australian Institute of International Affairs
32 Thesiger Court, Deakin ACT 2600, Australia
Phone: 02 6282 2133 Facsimile: 02 6285 2334
Website: www.aiia.asn.au; Email: ceo@aiia.asn.au

Preface

The Australian Institute of International Affairs (AIIA) was established in 1924 as an independent, non-profit organisation seeking to promote interest in, and understanding of, international affairs in Australia.

The AIIA provides a wide range of opportunities for the dissemination of information and free expression of views on these matters through discussion and publication. Precluded by its constitution from expressing any opinion of its own on international affairs, the AIIA provides a forum for the presentation, discussion and dissemination of a wide range of views.

The AIIA's series of Policy Commentaries aims to provide informed opinion and useful source documents on issues of topical concern to encourage debate amongst AIIA members, the media and the general public.

The Commentaries are edited by Melissa Conley Tyler, National Executive Director, in the AIIA National Office, Canberra. I hope that you will find the current commentary timely and informative.

Associate Professor Shirley Scott
Research Chair
Australian Institute of International Affairs
Series Editor 2010-2011

Editorial

Information and communication technology is disruptive technology. It tends to change the established way of doing things. From retail to journalism to routine social interaction, developments in information and communication technology (ICT) have had an enormous effect.

Because of this, there is a tendency to see new technologies in utopian or dystopian terms. Either new ICT will usher in a golden new age (for example, of 'people power' and democracy) – or it will inevitably lead to collapse and decay (for example, through debilitating cyberthreats). Sometimes there is little prediction between these extremes

This policy commentary focuses on the impact of ICT on international relations. It was decided to take a wide view of this relatively new area.

Dr Alison Broinowski comments on WikiLeaks from the perspective of a former Australian diplomat; she analyses the polarised and often immoderate reaction to WikiLeaks and its founder, Julian Assange. Fergus Hanson outlines the potential for ICT to assist the work of foreign ministries, particularly in public diplomacy, and the adaptation that will be required of them. Professor Anthony Billingsley evaluates the immediate and longer-term contribution of social media to the current wave of change in the Middle East and North Africa. Finally, Dr Myriam Dunn Cavelty identifies the pervasive narrative of cyberthreat and looks at the case of the Stuxnet worm; her conclusion is to focus on mitigation rather than succumb to fear of 'cyberdoom'.

Together these contributors aim to spark discussion, not to end it. ICT will continue to evolve, as will international relations in response. The impact of ICT is likely to fall somewhere between the utopias and dystopias that are currently imagined.

Melissa H. Conley Tyler
National Executive Director
Australian Institute of International Affairs

Remarks on Internet Freedom
US Secretary of State Hillary Rodham Clinton
21 January 2010*

[…] This is an important speech on a very important subject. […]

The spread of information networks is forming a new nervous system for our planet. When something happens in Haiti or Hunan, the rest of us learn about it in real time – from real people. And we can respond in real time as well. Americans eager to help in the aftermath of a disaster and the girl trapped in the supermarket are connected in ways that were not even imagined a year ago, even a generation ago. That same principle applies to almost all of humanity today. As we sit here, any of you – or maybe more likely, any of our children – can take out the tools that many carry every day and transmit this discussion to billions across the world.

Now, in many respects, information has never been so free. There are more ways to spread more ideas to more people than at any moment in history. And even in authoritarian countries, information networks are helping people discover new facts and making governments more accountable.

During his visit to China in November, for example, President Obama held a town hall meeting with an online component to highlight the importance of the internet. In response to a question that was sent in over the internet, he defended the right of people to freely access information, and said that the more freely information flows, the stronger societies become. He spoke about how access to information helps citizens hold their own governments accountable, generates new ideas, encourages creativity and entrepreneurship. The United States belief in that ground truth is what brings me here today.

* Available online (accessed 25 March 2011): http://www.state.gov/secretary/rm/2010/01/135519.htm

Because amid this unprecedented surge in connectivity, we must also recognize that these technologies are not an unmitigated blessing. These tools are also being exploited to undermine human progress and political rights. Just as steel can be used to build hospitals or machine guns, or nuclear power can either energize a city or destroy it, modern information networks and the technologies they support can be harnessed for good or for ill. The same networks that help organize movements for freedom also enable al-Qaida to spew hatred and incite violence against the innocent. And technologies with the potential to open up access to government and promote transparency can also be hijacked by governments to crush dissent and deny human rights.

In the last year, we've seen a spike in threats to the free flow of information. China, Tunisia, and Uzbekistan have stepped up their censorship of the internet. In Vietnam, access to popular social networking sites has suddenly disappeared. And last Friday in Egypt, 30 bloggers and activists were detained. One member of this group, Bassem Samir, who is thankfully no longer in prison, is with us today. So while it is clear that the spread of these technologies is transforming our world, it is still unclear how that transformation will affect the human rights and the human welfare of the world's population.

On their own, new technologies do not take sides in the struggle for freedom and progress, but the United States does. We stand for a single internet where all of humanity has equal access to knowledge and ideas. And we recognize that the world's information infrastructure will become what we and others make of it. Now, this challenge may be new, but our responsibility to help ensure the free exchange of ideas goes back to the birth of our republic. The words of the First Amendment to our Constitution are carved in 50 tons of Tennessee marble on the front of this building. And every generation of Americans has worked to protect the values etched in that stone.

Franklin Roosevelt built on these ideas when he delivered his Four Freedoms speech in 1941. Now, at the time, Americans faced a cavalcade of crises and a crisis of confidence. But the vision of a world in which all people enjoyed freedom of expression, freedom of worship, freedom from want, and freedom from fear transcended the troubles of his day. And years later, one of my heroes, Eleanor Roosevelt, worked to have these principles adopted as a cornerstone of the Universal Declaration of Human Rights. They have provided a lodestar to every succeeding generation, guiding us, galvanizing us, and enabling us to move forward in the face of uncertainty.

So as technology hurtles forward, we must think back to that legacy. We need to synchronize our technological progress with our principles. In accepting the Nobel Prize, President Obama spoke about the need to build a world in which peace rests on the inherent rights and dignities of every individual. And in my speech on human rights at Georgetown a few days later, I talked about how we must find ways to make human rights a reality. Today, we find an urgent need to protect these freedoms on the digital frontiers of the 21st century.

There are many other networks in the world. Some aid in the movement of people or resources, and some facilitate exchanges between individuals with the same work or interests. But the internet is a network that magnifies the power and potential of all others. And that's why we believe it's critical that its users are assured certain basic freedoms. Freedom of expression is first among them. This freedom is no longer defined solely by whether citizens can go into the town square and criticize their government without fear of retribution. Blogs, emails, social networks, and text messages have opened up new forums for exchanging ideas, and created new targets for censorship.

As I speak to you today, government censors somewhere are working furiously to erase my words from the records of history. But history itself has already condemned these tactics. Two months ago, I was in Germany to celebrate the 20thanniversary of the fall of the Berlin Wall. The leaders gathered at that ceremony paid tribute to the courageous men and women on the far side of that barrier who made the case against oppression by circulating small pamphlets called samizdat. Now, these leaflets questioned the claims and intentions of dictatorships in the Eastern Bloc and many people paid dearly for distributing them. But their words helped pierce the concrete and concertina wire of the Iron Curtain.

The Berlin Wall symbolized a world divided and it defined an entire era. Today, remnants of that wall sit inside this museum [The Newseum] where they belong, and the new iconic infrastructure of our age is the internet. Instead of division, it stands for connection. But even as networks spread to nations around the globe, virtual walls are cropping up in place of visible walls.

Some countries have erected electronic barriers that prevent their people from accessing portions of the world's networks. They've expunged words, names, and phrases from search engine results. They have violated the privacy of citizens who engage in non-violent political speech. These actions contravene the Universal Declaration on Human Rights, which tells us that all people have the right "to seek, receive and impart information and ideas through any media and regardless of frontiers." With the spread of these restrictive practices, a new information curtain is descending across much of the world. And beyond this partition, viral videos and blog posts are becoming the samizdat of our day.

As in the dictatorships of the past, governments are targeting independent thinkers who use these tools. In the demonstrations that followed Iran's presidential elections, grainy cell phone footage of a young woman's bloody murder provided a digital indictment of the government's brutality. We've seen reports that when Iranians living overseas posted online criticism of their nation's leaders, their family members in Iran were singled out for retribution. And despite an intense campaign of government intimidation, brave citizen journalists in Iran continue using technology to show the world and their fellow citizens what is happening inside their country. In speaking out on behalf of their own human rights, the Iranian people have inspired the world. And their courage is redefining how technology is used to spread truth and expose injustice.

Now, all societies recognize that free expression has its limits. We do not tolerate those who incite others to violence, such as the agents of al-Qaida who are, at this moment, using the internet to promote the mass murder of innocent people across the world. And hate speech that targets individuals on the basis of their race, religion, ethnicity, gender, or sexual orientation is reprehensible. It is an unfortunate fact that these issues are both growing challenges that the international community must confront together. And we must also grapple with the issue of anonymous speech. Those who use the internet to recruit terrorists or distribute stolen intellectual property cannot divorce their online actions from their real world identities. But these challenges must not become an excuse for governments to systematically violate the rights and privacy of those who use the internet for peaceful political purposes.

The freedom of expression may be the most obvious freedom to face challenges with the spread of new technologies, but it is not the only one. The freedom of worship usually involves the rights of individuals to commune or not commune with their Creator. And that's one channel of communication that does not rely on technology. But the freedom of worship also speaks to the universal right to come together with those who share your values and vision for humanity. In our history, those gatherings often took place in churches, synagogues, mosques and temples. Today, they may also take place on line.

The internet can help bridge divides between people of different faiths. As the President said in Cairo, freedom of religion is central to the ability of people to live together. And as we look for ways to expand dialogue, the internet holds out such tremendous promise. We've already begun connecting students in the United States with young people in Muslim communities around the world to discuss global challenges. And we will continue using this tool to foster discussion between individuals from different religious communities.

Some nations, however, have co-opted the internet as a tool to target and silence people of faith. Last year, for example, in Saudi Arabia, a man spent months in prison for blogging about Christianity. And a Harvard study found that the Saudi Government blocked many web pages about Hinduism, Judaism, Christianity, and even Islam. Countries including Vietnam and China employed similar tactics to restrict access to religious information.

Now, just as these technologies must not be used to punish peaceful political speech, they must also not be used to persecute or silence religious minorities. Now, prayers will always travel on higher networks. But connection technologies like the internet and social networking sites should enhance individuals' ability to worship as they see fit, come together with people of their own faith, and learn more about the beliefs of others. We must work to advance the freedom of worship online just as we do in other areas of life.

There are, of course, hundreds of millions of people living without the benefits of these technologies. In our world, as I've said many times, talent may be distributed universally, but opportunity is not. And we know from long experience that promoting social and economic development in countries where people lack access to knowledge, markets, capital, and opportunity can be frustrating and sometimes futile work. In this context, the internet can serve as a great equalizer. By providing people with access to knowledge and potential markets, networks can create opportunities where none exist.

Over the last year, I've seen this firsthand in Kenya, where farmers have seen their income grow by as much as 30 percent since they started using mobile banking technology; in Bangladesh, where more than 300,000 people have signed up to learn English on their mobile phones; and in Sub-Saharan Africa, where women entrepreneurs use the internet to get access to microcredit loans and connect themselves to global markets.

Now, these examples of progress can be replicated in the lives of the billion people at the bottom of the world's economic ladder. In many cases, the internet, mobile phones, and other connection technologies can do for economic growth what the Green Revolution did for agriculture. You can now generate significant yields from very modest inputs. And one World Bank study found that in a typical developing country, a 10 percent increase in the penetration rate for mobile phones led to an almost 1 percent increase in per capita GDP. To just put this into context, for India, that would translate into almost $10 billion a year.

A connection to global information networks is like an on-ramp to modernity. In the early years of these technologies, many believed that they would divide the world between haves and have-nots. But that hasn't happened. There are 4 billion cell phones in use today. Many of them are in the hands of market vendors, rickshaw drivers, and others who've historically lacked access to education and opportunity. Information networks have become a great leveler, and we should use them together to help lift people out of poverty and give them a freedom from want.

Now, we have every reason to be hopeful about what people can accomplish when they leverage communication networks and connection technologies to achieve progress. But make no mistake – some are and will continue to use global information networks for darker purposes. Violent extremists, criminal cartels, sexual predators, and authoritarian governments all seek to exploit these global networks. Just as terrorists have taken advantage of the openness of our societies to carry out their plots, violent extremists use the internet to radicalize and intimidate. As we work to advance freedoms, we must also work against those who use communication networks as tools of disruption and fear.

Governments and citizens must have confidence that the networks at the core of their national security and economic prosperity are safe and resilient. Now this is about more than petty hackers who deface websites. Our ability to bank online, use electronic commerce, and safeguard billions of dollars in intellectual property are all at stake if we cannot rely on the security of our information networks.

Disruptions in these systems demand a coordinated response by all governments, the private sector, and the international community. We need more tools to help law enforcement agencies cooperate across jurisdictions when criminal hackers and organized crime syndicates attack networks for financial gain. The same is true when social ills such as child pornography and the exploitation of trafficked women and girls online is there for the world to see and for those who exploit these people to make a profit. We applaud efforts such as the Council on Europe's Convention on Cybercrime that facilitate international cooperation in prosecuting such offenses. And we wish to redouble our efforts.

We have taken steps as a government, and as a Department, to find diplomatic solutions to strengthen global cyber security. We have a lot of people in the State Department working on this. They've joined together, and we created two years ago an office to coordinate foreign policy in cyberspace. We've worked to address this challenge at the UN and in other multilateral forums and to put cyber security on the world's agenda. And President Obama has just appointed a new national cyberspace policy coordinator who will help us work even more closely to ensure that everyone's networks stay free, secure, and reliable.

States, terrorists, and those who would act as their proxies must know that the United States will protect our networks. Those who disrupt the free flow of information in our society or any other pose a threat to our economy, our government, and our civil society. Countries or individuals that engage in cyber attacks should face consequences and international condemnation. In an internet-connected world, an attack on one nation's networks can be an attack on all. And by reinforcing that message, we can create norms of behavior among states and encourage respect for the global networked commons.

The final freedom, one that was probably inherent in what both President and Mrs. Roosevelt thought about and wrote about all those years ago, is one that flows from the four I've already mentioned: the freedom to connect – the idea that governments should not prevent people from connecting to the internet, to websites, or to each other. The freedom to connect is like the freedom of assembly, only in cyberspace. It allows individuals to get online, come together, and hopefully cooperate. Once you're on the internet, you don't need to be a tycoon or a rock star to have a huge impact on society.

The largest public response to the terrorist attacks in Mumbai was launched by a 13-year-old boy. He used social networks to organize blood drives and a massive interfaith book of condolence. In Colombia, an unemployed engineer brought together more than 12 million people in 190 cities around the world to demonstrate against the FARC terrorist movement. The protests were the largest antiterrorist demonstrations in history. And in the weeks that followed, the FARC saw more demobilizations and desertions than it had during a decade of military action. And in Mexico, a single email from a private citizen who was fed up with drug-related violence snowballed into huge demonstrations in all of the country's 32 states. In Mexico City alone, 150,000 people took to the streets in protest. So the internet can help humanity push back against those who promote violence and crime and extremism.

In Iran and Moldova and other countries, online organizing has been a critical tool for advancing democracy and enabling citizens to protest suspicious election results. And even in established democracies like the United States, we've seen the power of these tools to change history. Some of you may still remember the 2008 presidential election here.

The freedom to connect to these technologies can help transform societies, but it is also critically important to individuals. I was recently moved by the story of a doctor – and I won't tell you what country he was from – who was desperately trying to diagnose his daughter's rare medical condition. He consulted with two dozen specialists, but he still didn't have an answer. But he finally identified the condition, and found a cure, by using an internet search engine. That's one of the reasons why unfettered access to search engine technology is so important in individuals' lives.

Now, the principles I've outlined today will guide our approach in addressing the issue of internet freedom and the use of these technologies. And I want to speak about how we apply them in practice. The United States is committed to devoting the diplomatic, economic, and technological resources necessary to advance these freedoms. We are a nation made up of immigrants from every country and every interest that spans the globe. Our foreign policy is premised on the idea that no country more than America stands to benefit when there is cooperation among peoples and states. And no country shoulders a heavier burden when conflict and misunderstanding drive nations apart. So we are well placed to seize the opportunities that come with interconnectivity. And as the birthplace for so many of these technologies, including the internet itself, we have a responsibility to see them used for good. To do that, we need to develop our capacity for what we call, at the State Department, 21st century statecraft.

Realigning our policies and our priorities will not be easy. But adjusting to new technology rarely is. When the telegraph was introduced, it was a source of great anxiety for many in the diplomatic community, where the prospect of receiving daily instructions from capitals was not entirely welcome. But just as our diplomats eventually mastered the telegraph, they are doing the same to harness the potential of these new tools as well. […]

In a short span, we have taken significant strides to translate the promise of these technologies into results that make a difference. But there is still so much more to be done. And as we work together with the private sector and foreign governments to deploy the tools of 21st century statecraft, we have to remember our shared responsibility to safeguard the freedoms that I've talked about today. We feel strongly that principles like information freedom aren't just good policy, not just somehow connected to our national values, but they are universal and they're also good for business. […]

Now, pursuing the freedoms I've talked about today is, I believe, the right thing to do. But I also believe it's the smart thing to do. By advancing this agenda, we align our principles, our economic goals, and our strategic priorities. We need to work toward a world in which access to networks and information brings people closer together and expands the definition of the global community. Given the magnitude of the challenges we're facing, we need people around the world to pool their knowledge and creativity to help rebuild the global economy, to protect our environment, to defeat violent extremism, and build a future in which every human being can live up to and realize his or her God-given potential.

So let me close by asking you to remember the little girl who was pulled from the rubble on Monday in Port-au-Prince. She's alive, she was reunited with her family, she will have the chance to grow up because these networks took a voice that was buried and spread it to the world. No nation, no group, no individual should stay buried in the rubble of oppression. We cannot stand by while people are separated from the human family by walls of censorship. And we cannot be silent about these issues simply because we cannot hear the cries.

So let us recommit ourselves to this cause. Let us make these technologies a force for real progress the world over. And let us go forward together to champion these freedoms for our time, for our young people who deserve every opportunity we can give them.

Thank you all very much.

WikiLeaks Announcement: Secret US Embassy Cables

28 November 2010[*]

Wikileaks began on Sunday November 28th publishing 251,287 leaked United States embassy cables, the largest set of confidential documents ever to be released into the public domain. The documents will give people around the world an unprecedented insight into US Government foreign activities.

The cables, which date from 1966 up until the end of February this year, contain confidential communications between 274 embassies in countries throughout the world and the State Department in Washington DC. 15,652 of the cables are classified Secret.

The embassy cables will be released in stages over the next few months. The subject matter of these cables is of such importance, and the geographical spread so broad, that to do otherwise would not do this material justice.

The cables show the extent of US spying on its allies and the UN; turning a blind eye to corruption and human rights abuse in "client states"; backroom deals with supposedly neutral countries; lobbying for US corporations; and the measures US diplomats take to advance those who have access to them.

This document release reveals the contradictions between the US's public persona and what it says behind closed doors – and shows that if citizens in a democracy want their governments to reflect their wishes, they should ask to see what's going on behind the scenes.

[*] Available online (accessed 25 March 2010): http://wikileaks.ch/cablegate.html

Every American schoolchild is taught that George Washington – the country's first President – could not tell a lie. If the administrations of his successors lived up to the same principle, today's document flood would be a mere embarrassment. Instead, the US Government has been warning governments -- even the most corrupt -- around the world about the coming leaks and is bracing itself for the exposures.

The full set consists of 251,287 documents, comprising 261,276,536 words (seven times the size of "The Iraq War Logs", the world's previously largest classified information release).

The cables cover from 28th December 1966 to 28th February 2010 and originate from 274 embassies, consulates and diplomatic missions. [...]

Attorney-General the Hon Robert McClelland MP: Doorstop on leaking of US classified documents by Wikileaks

29 November 2011*

ROBERT MCCLELLAND: Obviously the leaking of this substantial amount of information is a real concern to Australia. Every indication is that some of the documentation could relate to national security classified documentation; we are waiting to assess the full extent of that. We have had some discussions across ministers, of course, with various United States officials, including the United States Ambassador, who's been very helpful and cooperative.

It is a matter that is taken with the utmost seriousness by the government of the United States and certainly the government of Australia and obviously governments around the world.

The release of this information could prejudice the safety of people referred to in the documentation and indeed, could be damaging to the national security interests of the United States and its allies, including Australia. So obviously Australia will support any law enforcement action that may be taken. The United States will be the lead government in that respect, but certainly Australian agencies will assist and we will look at - of course, I'd ask the Australian Federal Police to look at the issue as to whether any Australian laws have been breached as a specific issue as well.

So, these are serious matters; and we have formed a whole-of-government taskforce to look at the issues. There had previously been a specific Defence taskforce looking at a Defence documentation, but

* Available online (accessed 25 March 2010): http://www.ag.gov.au/www/ministers/mcclelland.nsf/Page/Transcripts_2010_FourthQuarter_29November2010-DoorstoponleakingofUSclassifieddocumentsbyWikiLeaks

obviously, the documentations in so far, it suggested, could relate to issues broader than simply Defence strategy.

There has been established a whole-of-government taskforce to look at those issues and to obviously go through each and every incident to see what impact it may have and what action should appropriately be taken to firstly reduce any impact - adverse impact, but certainly to see what can be done to rectify the situation.

The Hon Julia Gillard MP, Prime Minister of Australia Transcript of Interview with Gary Hardgrave, 4BC

2 December 2010[*]

[…] HOST: Wikileaks, what should we be worried about, you'd have had the briefing by now, what are they telling you we should be waiting for?

PM: Look I have been receiving briefings and we have a whole process to go through all of this information, I mean, millions of pieces of information and asses the implications for us. So we'll work through that and I absolutely condemn the placement of this information on the Wikileaks website, it's a grossly irresponsible thing to do, and an illegal thing to do.

HOST: It's going to be interesting to see where that ultimately goes and Queensland's claiming Mr Assange and his mother's a little bit terrified and disappointed and worried about him, Australia I guess will have some say when people catch up to him as to what happens to him I would hope we'd have some say.

PM: You can always understand a mother's love and anxiety about her son and I do understand that, but the wrong thing's been done here.

[*] Available online (accessed 25 March 2010): http://www.pm.gov.au/press-office/transcript-interview-gary-hardgrave-4bc

Australian Federal Police Media Statement: Finalisation of WikiLeaks referral

17 December 2010[*]

On 30 November the Attorney-General's Department referred the matter relating to the publishing of United States (US) embassy cables containing classified information on the WikiLeaks website to the Australian Federal Police.

The AFP examined material relevant to potential Australian offences to determine whether an official investigation was warranted.

The AFP has completed its evaluation of the material available and has not established the existence of any criminal offences where Australia would have jurisdiction.

Where additional cables are published and criminal offences are suspected, these matters should be referred to the AFP for evaluation.

[*] Available online (accessed 25 March 2011): http://www.afp.gov.au/media-centre/news/afp/2010/december/finalisation-of-wikileaks-referral.aspx

Interview with Minister for Foreign Affairs the Hon Kevin Rudd MP by Fran Kelly, ABC Radio National

21 February 2011[*]

[…] KEVIN RUDD: The first thing I'd say is that it is a tired but predictable script to be used in various parts of the Middle East to blame what is occurring on the streets of various Middle Eastern capitals on external interference. This is not external interference.

What we find is that the people of Libya - like the people of so many other countries around the region - are finding a voice. They have connected with one another through the new media, through social media. Libya has been particularly impacted by what has occurred through its near neighbour, Tunisia, in North Africa. And therefore, what we see is people saying that their rights to freedom of expression should be respected as they understand them to be respected in so many other parts of the world.

On the question of the future of the Libyan regime, there are conflicting reports in terms of the internal stability of the regime; obviously, our analytical community together with others are watching events closely.

FRAN KELLY: Have you been surprised by, let's call it the contagion, this - of pro-democracy movements standing up across the region, across Africa, across the Middle East? Do you think it's unstoppable now?

KEVIN RUDD: I think, Fran, I'd disagree with the word contagion that tends to infer something which is by definition, bad. […] Can I just say people are responding to basic impulses in all members of the human family, which is the right to freedom of expression, the right to

[*] Available online (accessed 25 March 2011): http://www.foreignminister.gov.au/transcripts/2011/kr_tr_110221_radio_national.html

participate in the national political life of a country, the right for freedom of association. And these know no bounds, as I've said repeatedly; they are not constricted to a culture, a country, a society, or at a particular time.

What differs across the world are the individual national circumstances which will obviously make it slower or more difficult in various parts of the world for these aspirations to be realised.

Remember in the West, what we call the West, hard-won democratic freedoms were the product of sometimes one and two centuries of struggle.

FRAN KELLY: So do you expect that it is unstoppable now? Is that what you're saying?

KEVIN RUDD: No, what I'm saying is that this is a universal aspiration. If you look at the younger generation in particular, those under 30, and the resort to the new technologies, people's experiences are now being shared right across the Middle East.

Also, let's not underestimate the impact of Al Jazeera, the television station which broadcasts consistently and continually right across the neighbourhood bringing people fresh images of protest, peaceful protest, in some cases successful protest, in various other capitals of the world.

[…]

Interview with Australian Minister for Foreign Affairs Kevin Rudd by Heather Ewart, ABC Television

21 February 2011[*]

[...] HEATHER EWART: Did the CIA and other intelligence agencies, including ours, see this coming; and if not, why not?

KEVIN RUDD: Well, Heather, you know what the convention is; we never discuss the contents of intelligence information, either our own or that which we share with partners around the world.

Let me answer your question a different way. I think more broadly analysts failed to grasp the depth of the social movement that was underway in the Arab world. Let's just be blunt about it.

And to be fair to those who work professionally in this area, it's always difficult to get a handle on what's happening in the proverbial Arab street, when you've got not just a huge youth demographic, for example in Egypt, but the proliferation now of new social media communications, which enable the turbo-charging of social movements.

But even in the absence of that, 20 years ago most of the analytical community, for example, got it wrong when it came to Tiananmen in China.

And so let's just be clear about this: the challenge now, given the new realities, is how do we support the interim Egyptian government and the Egyptian people in what is going to be a very difficult process of transition between now and the end of the year?

[*] Available online (accessed 25 March 2011): http://www.foreignminister.gov.au/transcripts/2011/kr_tr_110221_730_report.html

HEATHER EWART: Because of course it's not just Libya; there's a wave of pro-democracy protests going on throughout this region. Is it possible that the results could not always be what the Western world wants?

KEVIN RUDD: Well, entirely. I made some remarks on this in the Australian Parliament today. We welcome and celebrate the cry for freedom, and it's real. Young people in these countries want to have the same freedom of expression that we are enjoying on this television program right now, and to have that reflected in their political processes formally as well. But on the other hand, what you also face is some genuine concerns. For example, if democratic processes are used and abused by effectively non-democratic forces, then obtain power and then roll back the freedoms which have been so secured, we have a problem. Look at the Iranian regime as the classic case study.

So, why do I say this? It's imperative that we in the international community work to support Egypt, the biggest state in the region, with practical areas of assistance, food security, various job programs, as well as other forms of practical help, and it's a critical year ahead. If it goes wrong, it could go really wrong. [...]

Julian meets Julia: WikiLeaks and Australian Diplomacy

Dr Alison Broinowski*

The Internet has changed the way we live and communicate. How radically and rapidly this has happened in diplomacy is demonstrated by WikiLeaks and Julian Assange. Their names, that in mid-2010 were still unfamiliar to most of us, were receiving millions of hits on Google by December, when Mark Zuckerberg only narrowly beat the 39-year-old Australian to become *Time*'s person of the year. Among the wired around the world, the two geeks had been famous for much longer, one as the founder of Facebook and the other, before he set up WikiLeaks, as a cyber-activist and collaborator in a 1997 book about hacking.[1] Zuckerberg has made a fortune and there is already a film (*The Social Network*, 2010) about him; Assange is the subject of at least five books, including his own, and one film, with more on the way.[2] (Consider several of the words used in this paragraph: even a year ago, would such expressions have appeared in an article on foreign policy?).

Assange's rapid rise to prominence reflects the supply of information and the demand for its instant delivery that drive electronic journalism. His first big coup was in April 2010 when WikiLeaks published US military footage of the deliberate shooting of Iraqi civilians and Reuters journalists from a helicopter. Then he offered three large 'dumps' of classified US government documents that, at a time of decline in newspaper readership and profitability, were irresistible to the media. The five papers which partnered with Assange received US military files on the war in Afghanistan in July, followed by more on Iraq in October. Then, in November, he delivered 251,000 US State Department cables,

[*] Dr Alison Broinowski is a former Australian diplomat, Visiting Fellow at the Australian National University and Senior Research Fellow at the University of Wollongong.

of which they have so far published only a few thousand. *The Guardian*, *The New York Times*, *Le Monde, Der Speigel,* and *El Pais* are still sitting on a bag of potential cash, if not a time bomb. Of course, they had to spend considerable resources on editing the material, and on getting up to speed with the technology, and none of them has said if or how much Assange was paid; it is unlikely that the drinks and late night dinners shouted for him by *The Guardian* were his only recompense. *The Age* and *The Sydney Morning Herald*, which have been running stories based on the cables relating to Australia, are among some 60 papers receiving selected material, and in their case too, whether chequebooks came out for it is not clear. Press freedom is not entirely free. To have beaten the Murdoch papers, that always love an 'exclusive', may be Fairfax's greatest reward. What is certain is that WikiLeaks has much more material yet to dribble out on US foreign affairs and defence, involving Australia and many other countries. WikiLeaks Cable Viewer is producing more revelations. Assange and WikiLeaks seem set to continue as an evolving story so fascinating that, as *The Guardian's* writers said, you couldn't make it up.[3]

Let us first consider WikiLeaks, and then its enigmatic founder. How significant are they? The answer depends on who you are and how they affect your interests.

In the past year, reactions to WikiLeaks in Australia and in most other countries have ranged from outrage to ecstasy. As I have suggested, editors who are on the newsfeed love it, and so, presumably, do many of their readers. Most governments hate it, and their confused responses to this new phenomenon appear to be made up on the run. They can hardly admit that a free press is the last thing they want. How can any country that has signed the International Convention on Civil and Political Rights, or has freedom of expression in its constitution, ban WikiLeaks? The Murdoch media are not banned for their leaked 'exclusives'. The Pentagon, after television turned public opinion against the Vietnam War, hit on the idea of embedding journalists; in Iraq, it thought it had that war firewalled. Americans invented the internet, and should have known before the Abu Ghraib revelations what dangerous power it had.

The concern they now express for the safety of Iraqis or Afghanis named in the cables, after innocent civilians have frequently and carelessly been killed by their own troops and sometimes by their allies, is scarcely a convincing argument against WikiLeaks. *The Guardian*'s authors say they know of no retribution against people whose names were not redacted.[4]

Prime Minister Julia Gillard was quick to declare Assange's activities "illegal", but neither she nor the Attorney-General, Robert McClelland, could say under what law. In response to a suggestion from Assange himself that she had passed information about people working for WikiLeaks to the United States, she denied any knowledge of it.[5] Secretary of State Hillary Clinton in January 2010 endorsed semi-underground digital publishing as the potential "new nervous system for our planet", and in February announced $US25 million to help people in China and elsewhere to "get around filters, stay one step ahead of the censors" and fight against "Internet repression"[6] but reversed herself just before the State Department cables were published, denouncing digital transparency as "an attack on the international community", and WikiLeaks as "a danger to the world". Public morality, it seems, is not only subjective, but reversible. Other prominent Americans have invoked treason without explaining how an Australian citizen, or an organisation based in Sweden, can commit it against the United States.

Foreign Minister Kevin Rudd, less out of his depth, has asserted that legal liability rests with the American or Americans who leaked the material. Governments, said Rudd, should be able to deal with each other in secrecy. The more cables about him emerge, the more understandable his wish for discretion becomes. However much of what we have seen about him is rather trivial and out of date: take as examples Prime Minister Rudd's crack to Bush about Queensland being bigger than Texas; his reported last-minute cancellation of a trip to Washington; and talk of his reputation in Canberra as a control freak. Moreover, to people accustomed to reading diplomatic cables, little of the State Department reporting is surprising, nor is the fact that they contain a mere 1400 mentions of Australia. Some of the content either originated in the media in the first place or has later appeared there: for instance Rudd being asked by Bush what the G20 is, and China's official comment on the 2009 Defence White Paper as 'crazy' and 'dangerous'. More surprising to observers outside government, perhaps, is the eager intimacy of Australians with US diplomats that appears at times to reflect misplaced national identity.

Assessments of leaders' personal peccadilloes are a staple of diplomatic discourse, and are more entertaining than they are shocking, unless of course it is you who is named. Serving diplomats defend the continuing necessity of confidentiality in certain circumstances.[7] They will now, no doubt, be more circumspect in what they say to foreign colleagues, at least until things settle down and business returns to near-normal, as it will. They may feel a degree of *schadenfreude* at the spectacle of the US NOFORN ('not for release to non-Americans') restriction leaking like a drain, particularly if their own governments have in the past been castigated by the United States for some lapse of security. They may enjoy receiving explanations hastily offered by US diplomats for cables that haven't even appeared. The State Department has found the cables' release sufficiently embarrassing to undertake damage containment in several capitals, with Hillary Clinton herself delivering apologies to some governments, and ambassadors offering excuses to others (such as Australia). But these cables date back at least to 2003, and they lose newsworthiness with every passing day. Moreover – and this is what is least appreciated about the cables– none of them is classified higher than confidential, so the State Department's secret and top secret material remains secure. The media love to exaggerate the significance of their scoops; they don't admit that the WikiLeaks diplomatic dump is a glass half-full.

Everyone reading it, naturally, finds plenty in it to interest them. *The Guardian*'s writers are drawn to Assange by his revelations from 2007 about three cases related to Britain: the corruption of former Kenyan president Daniel Arap Moi, Barclays Bank's tax avoidance schemes and toxic waste dumping by the oil trader Trafigura. The editors of *El Pais* discover that the US Embassy in Madrid tried to influence judges, prosecutors and the government in cases involving US citizens not only in Spain but also in Latin American countries, where these revelations have been published to considerable effect.[8] The Indonesian government is outraged by a succession of State Department cables between 2004 and 2010 alleging corruption by President Susilo Bambang Yudhoyono, his wife and family, and a union in Jakarta is now suing *The Sydney Morning Herald* and *The Age* for $1 million for publishing these allegations in March 2011. Young people in the Middle East and North Africa read the evidence of the corruption of their leaders from WikiLeaks, and the flame of revolt ignited by a protest suicide in Tunisia in November 2010 spreads rapidly, with momentous consequences there and in Egypt, Morocco, Yemen, Libya, Bahrain and Syria. The wired young, already active in the Middle East and North Africa, are quick to spread the word, and can mobilise in hours.[9] US diplomatic embarrassment is one thing: the overthrow of some of its long-standing cronies in the name of democracy is quite another.[10]

In Australia, the press delivers other reality checks from WikiLeaks. We now know, for example, that:

- senior people in ONA have for years considered Afghanistan a lost cause, in spite of prime ministers saying Australian troops would stay there for years and finish the job;
- at least one minister is urging selling uranium to India and developing nuclear power in Australia, while the government publicly denies both policies;
- the 2009 Defence White Paper's reservations about Missile Defence are intended to placate the Left, while the government continues working with the United States on Missile Defence at Pine Gap;
- Australian strategic analysts, who used to advise the United States against containing China, from 2010 took a more aggressive line, urging the possible use of force;
- Rudd's proposed Asia Pacific community was intended to curb the growing influence of China and keep the United States involved in Asia;

- as acting Prime Minister in December 2008, Gillard reversed Australia's position on Israel's attack on Gaza and sought an early opportunity, which she later took up, to visit Israel;
- the United States does keep body counts of enemies and civilians in Iraq and Afghanistan, having denied this since 2002; and
- in December 2008 the International Atomic Energy Agency identified 'a serious problem' with nuclear reactors in Japan, where recent earthquake levels were higher than facilities were designed to withstand.

These revelations – that for insiders merely serve as confirmations – nonetheless show up things that the mainstream media do not tell us. However the leak-publishing process itself has been haphazard from the start. The original cable dump, huge as it is, may be incomplete; WikiLeaks arbitrates on what to deliver from it and what to withhold; the editors of the five partner newspapers further filter the cables, redacting some references as they see fit; and finally Fairfax dribbles out whatever it decides the Australian public, at the end of the food chain, needs to know. So this is hardly the full story, nor is it freedom of information: perhaps some FOI applications are needed from readers to Fairfax. For my part, I would particularly like to see the cables in full, not just the lines cited in the press. I am curious to know what they say about Rudd's Nuclear Non-Proliferation and Disarmament Conference, the death of British nuclear scientist Dr David Kelly and Australia's part in the Oil for Food Program in Iraq – and why all three trails have gone cold. If ancient history could be dug up, it would be interesting to read US comments on the Adelaide to Darwin railway, or the Hilton Hotel bombing or Robert Menzies' offer to send troops to Vietnam – or even the dismissal of Gough Whitlam. However I expect to be disappointed, because these are not in the dump, and in any case they would be classified higher than confidential.

Now for Julian Assange. What he and his organisation specialise in doing is inspired by the old I.F. Stone adage: *governments lie*. Because he reveals the lies governments – including Australia's – have told to others and to their own people, Assange attracts the same extremes of disgust and adulation as WikiLeaks does. He is to US Vice President Joe Biden "a high-tech terrorist",[11] and to Julia Gillard anarchic and amoral. With his obvious intelligence, striking appearance, idiosyncratic modes of expression, unconventional upbringing and exotic surname (from his stepfather, supposedly the descendant of a 19th century Chinese settler in Queensland, Ah Sang), he is manna from heaven for the media. His detractors point to his conviction for hacking in 1996 after he and others in Melbourne accessed US defence sites and ANU computer systems (for which he was fined but not jailed). Others note with distaste his erratic education and failures in various university courses. Robert Manne traces his association in the 1990s with the 'Cypherpunks' group who pioneered public-key cryptography, seeking to enable individuals to communicate confidentially and cost-free. Two individuals on the list even advocated 'assassination markets' encouraging citizens to contribute to a lottery whose jackpot went to the person who predicted the assassination of certain politicians or 'Congressrodents' – by carrying it out. [12] After 2002, Assange ceased to be a cypherpunk cryptoanarchist, but maintained his contempt for Western political and economic elites and the mainstream media. Along the way he lost friends, some of whom now say he is greedy and narcissistic, an irresponsible father and uncouth in dress, personal and sexual habits. Whether in those respects he is better or worse than many politicians, diplomats and journalists is another matter of personal perspective.

Assange's adulators are drawn to his conviction and idealism. "If we can only live once", he writes, "then let it be a daring adventure that draws on all our powers…The whole universe…is a worthy opponent, but try as I may I cannot escape the sound of suffering…Men in their prime, if they have convictions, are tasked to act on them".[13] In December 2006, just before launching WikiLeaks, he emailed Daniel Ellsberg, who became a supporter: "We have come to the conclusion that fomenting a worldwide movement of mass leaking is the most cost effective political intervention". His targets are oppressive regimes in Asia, the former Soviet bloc, sub-Saharan Africa and the Middle East, and his Western supporters include those 'who wish to reveal unethical behavior in their own governments and corporations'. [14] Assange's notion of 'scientific journalism' appeals to the growing number of people who mistrust the mass media, and who see him as opening otherwise unaccountable institutions to public scrutiny and changing them. His forthcoming book is no less ambitious: he wants it to become "one of the unifying documents of our generation…explain[ing] our global struggle to force a new relationship between the people and their governments". John Pilger (who if he were one of this generation might have been another Assange) credits WikiLeaks with demonstrating that reality is no longer what governments and the media say it is:[15] in other words, that both governments and the mainstream media lie. Robert Manne sees WikiLeaks as so significant that he identifies Murdoch and Assange as "the two most influential Australians of the era".[16]

The cogs of justice are slowly grinding towards delivering Assange to Sweden to face dubious charges in an erratic legal process. According to Naomi Wolf, men are pretty much never treated the way Assange is being treated in the face of sex crime charges.[17] The Pentagon began a campaign against WikiLeaks three years ago, threatening exposure and criminal prosecution, and the US has forced the Bank of America and credit card agencies to stop delivering payments to WikiLeaks. With a compliant government in Sweden (allegedly now advised by former Bush staff member Karl Rove[18]), the United States may succeed in getting Assange extradited, perhaps to face the conditions of imprisonment which President Obama has described as 'appropriate' for Bradley Manning, the suspected leaker. Prime Minister Gillard has denounced Assange, apparently allowing her loyalty to the United States to override her duty to protect an Australian citizen abroad and to uphold the presumption of his innocence. At least she has since asserted that Australia will not allow extradition to countries with the death penalty. However the record of Labor in government in the cases of Mamdouh Habib, David Hicks and Mohammed Haneef that it inherited from John Howard, does not inspire confidence.

The interest in watching Prime Minister Gillard try to extricate herself from her contradictory statements is only one reason why the evolving story of Assange and WikiLeaks will continue to attract millions of hits.

It raises important questions of principle that apply to governments all over the world that are signatories of the International Convention on Civil and Political Rights.

[1] Suelette Dreyfus, *Underground: tales of hacking, madness & obsession on the electronic frontier* (Melbourne: Reed Books Australia, 1997).

[2] Daniel Domscheit-Berg, *Inside WikiLeaks – my time with Julian Assange at the world's most dangerous website* (Melbourne: Scribe, 2011); Julian Assange, *WikiLeaks vs. the World* (Melbourne: Text, 2011); Andrew Fowler, *The Most Dangerous Man* (Melbourne: Melbourne University Press, 2011); *In the Realm of the Hackers,* documentary film, Kevin Anderson, 2003; *WikiLeaks: the Movie*, forthcoming film, Stephen Speilberg.

[3] David Leigh and Luke Harding, *WikiLeaks: inside Julian Assange's War on Secrecy* (London: Guardian Books, 2010).

[4] Ibid.

[5] *Q&A*, ABC TV, 14 March 2011, available online: http://www.abc.net.au/tv/qanda/txt/s3157403.htm (accessed 28 March 2011).

[6] Hillary Clinton quoted by Perry Link, 'How China fears the Middle East Revolutions', *The New York Review of Books* (24 March 2011, pp. 21-2).

[7] John McCarthy, 'WikiLeaks', *The Asialink Essays 2011*, Vol.3, No.1, http://www.asialink.unimelb.edu.au/publications/the_asialink_essays (accessed 28 March 2011)

[8] Leigh and Harding, op. cit., p. 127.

[9] Max Rodenbeck, 'Volcano of Rage', *The New York Review of Books,* 24 March 2011, pp. 4-7 ; Perry Link, op. cit., pp. 21-22.

[10] US Secretary of State Hillary Rodham Clinton has linked the "new technologies of the 21st century" with the "Arab Spring" in her remarks at the Human Rights Council, 28 February 2011, available online: http://www.state.gov/secretary/rm/2011/02/157412.htm (accessed 28 March 2011). Julian Assange denies this, saying Egyptian insurgents warned each other against using the internet, and that Al Jazeera was more influential: 'Julian Assange speaks to Union', 15 March 2011, available online: http://www.varsity.co.uk/news/3494 (accessed 28 March 2011).

[11] Lucy Bannerman, 'Assange a high-tech terrorist: Biden', *The Australian,* 20 December 2010, available online:

http://www.theaustralian.com.au/news/world/assange-a-high-tech-terrorist-biden/story-e6frg6so-1225973696881 (accessed 28 March 2011).

[12] Robert Manne, 'The Cypherpunk Revolutionary: Robert Manne on Julian Assange', *The Monthly*, March 2011, pp. 17-35.

[13] Quoted in Manne, ibid.

[14] Preceding quotes in this paragraph from Leigh and Harding, op. cit., pp.47-8

[15] John Pilger, speech to Sydney Peace Foundation, Sydney, 16 March 2011, available online: http://www.johnpilger.com/videos/breaking-australias-silence-WikiLeaks-and-freedom (accessed 28 March 2011).

[16] Manne, op. cit., p. 35.

[17] Naomi Wolf, 'J'Accuse: Sweden, Britain, and Interpol Insult Rape Victims Worldwide', *Huffington Post*, 13 December 2010, available online: http://www.huffingtonpost.com/naomi-wolf/jaccuse-sweden-britain-an_b_795899.html (accessed 28 March 2011).

[18] Johan Nylander, 'Karl Rove behind Sweden's hunt for Assange?', *Swedish Wire*, 12 January 2011, available online: http://www.swedishwire.com/component/content/article/2-politics/8048-karl-rove-behind-swedens-hunt-for-assange (accessed 28 March 2011).

The New Public Diplomacy

Fergus Hanson[*]

As recently as November last year Eric Schmidt, CEO of Google, told the Council on Foreign Relations "I think most people don't appreciate how fast this mobile phenomenon is going to occur, especially outside of the developed world".[1] If anyone was underestimating the spread of these tools it only took the social media-infused revolutions in Tunisia and Egypt a few months later to spell out how wired the world has become and how unpredictable the uses of social media will be. For public diplomacy practitioners it served as a reminder: the world has undergone some rapid and dramatic changes that require them to adapt quickly.

The numbers Schmidt was talking about are simply extraordinary. The world now has somewhere between four and five billion mobile phones; and nearly one billion of them are smart phones with some capacity to access the internet, like iPhones and Blackberries. And because of their rapidly declining cost, Google expects another one billion people to join these web-enabled networks in just the next two to three years.[2] That is a population the size of China's, suddenly being connected to a global network that gives them access to the sum of all human knowledge and the capability to connect with millions of other people in the space of three years.

In fact, smart phones are predicted to overtake desktop computers as the preferred means of accessing the web somewhere between 2013 and 2014.[3] Internet penetration rates have also been increasing dramatically over the last decade, from less than half a billion users in 2000 to around two billion in 2010. [4]

[*] Fergus Hanson is the Director of Polling and a Research Fellow at the Lowy Institute of International Policy.

As if that were not enough of a disruption, add in the demographics as well. The majority of the world's population is under 30 years of age, and in the developing world the proportion under 30 is even larger. These are the people who have grown up seamlessly integrating these new technologies into their daily lives.

These are some of the mega-trends changing the behaviour of everyone from bankers to peasant farmers. Public diplomacy practitioners are not exempt.

Until very recently it was not uncommon to hear people scoff at Twitter. What on earth could you do with a 140-character message? For many it was just another example of inane Western narcissism. However, after the central organising role social media has played in many of the recent protests across the Middle East and North Africa, critics of social media have been noticeably quieter. The point is not just that some people have underestimated the change that is afoot as a result of a networked world, it is also that predicting how these tools will be used is incredibly difficult. Facebook was not invented to help topple regimes.

Yet while it might be hard to predict specific outcomes of this change, it does seem possible to draw out some of the major implications for public diplomacy practitioners. Here are three.

New Communications Platforms are Different

First, social media platforms appear to be qualitatively different from other communications technologies we have seen in the past, which means diplomats can and should be reaching much bigger audiences. It also means they will be competing for a voice in a much more crowded space.

Other communications technology revolutions like the printing press, radio and television – while facilitating communication with mass audiences – still operated under a hierarchical structure where gatekeepers regulated the number of voices that could be heard and who could be heard.

New digital communication platforms like Twitter, Facebook and blogs are far more democratic. In what will be an incredibly short timeframe, the world will soon reach the point where almost every single person on the planet has the potential to be a publisher, writer, photographer, video producer and blogger. What is more, the communications system is now networked; this means that someone like P.J. Crowley, the former U.S. Assistant Secretary of State for Public Affairs, who has around 26,000 Twitter followers, can still reach millions of people through re-tweets and the network effects that Twitter enables.[5] The individual has been empowered like never before.

These tools also allow diplomats on the ground to reach much bigger audiences. No longer are a few hundred contacts sufficient. With social media, a single diplomat at the US Embassy in Jakarta is reaching more than 300,000 Indonesians through the Embassy's Facebook account.[6] According to a cable recently released by WikiLeaks the Embassy in Jakarta is also growing its audiences through sophisticated digital campaigns.[7]

Attracting mass social media followings in such a crowded space is not easy and requires adaptation. Carefully vetted messages will not work in an information-saturated environment. The stuffiness and traditional inaccessibility of diplomacy needs to be discarded in this online space, where engagement and interactivity are key. That involves foreign ministries trusting their staff online just as much as they trust them to negotiate major international deals behind closed doors.

Audiences and Debates are Moving Online

Each time I visit North America, I am amazed how frequently area experts cite blog posts in conversation or during formal public discussions. Here in Australia, even though this shift is still in progress, increasingly, audiences and debates have moved online. If foreign ministries do not adjust the way they communicate then increasingly they won't be heard.

Take the example of Islamic extremism. Western countries are spending billions countering this threat in a variety of ways; Australia has deployed forces to both Iraq and Afghanistan. It is received wisdom that Islamic extremists are using the internet to radicalise youth. Despite this, only a handful of Western governments are present in the online space. The State Department has nine full-time Arabic-language bloggers, two Farsi bloggers and two Urdu bloggers, for example. The Pentagon and UK Foreign and Commonwealth Office also maintain full-time bloggers.[8] But given the modest cost of this sort of campaigning compared to the potential benefits, it seems odd that more governments are not working to counter these threats online.

Beyond the narrow world of extremism, there are other reasons public diplomacy campaigners need to be online. A big reason is that increasingly that is where national and international debates are taking place. During a visit last year to the headquarters of a major international newsgroup I was surprised when one of its 60-something year-old editors pulled out his blackberry to show me news items rolling in on his Facebook news feed. Through the feed he was connected with all the leading opinion-makers within his bailiwick, from ambassadors to politicians, business leaders to think-tankers. It alerted him to developments as they happened and also provided context and nuance to news he would otherwise have only seen via press release or a transcript.

The point I took was that public debates and positions are shaping up well before they hit newspapers. Governments that are not even feeding into this discussion are unnecessarily impeding any chance they have of shaping the debate.

The recent protests in Egypt were a good example. In the early stages, the commentary from the US government on the protests seemed ambiguous. Not surprisingly, these early remarks caused a stir on

Twitter. What was fascinating, though, was the response of US officials, who apparently saw the negative tone the remarks were generating and immediately started spinning official government comments in a more positive light. These employees are connected through their followers with all the major US and international media, giving them a chance to shape the tone of reporting well before a single newspaper hit the newsstands or a considered blog post was up.

It is debatable how effective these efforts were in framing the subsequent considered comment, but it would seem counterproductive to US interests for its officials not to be trying their best both to put and clarify the government's view.

The challenge for foreign ministries is that these networks cannot be built overnight. They take time to grow and require continuous cultivation to maintain. So if Australia's Department of Foreign Affairs and Trade (DFAT) wants to be able to harness these tools in a crisis situation, it needs to be using and building the networks continuously. As the Egypt example highlights, waiting until newspapers have gone to print is now too late. The implications of a policy or speech have already been debated for hours by expert minds across the globe. As the Prime Minister Julia Gillard put it:

> Something that was a blockbuster at 10 a.m. when it's announced has been tweeted about by 10.05, has been blogged about by 10.30....That's the nature of the cycle and I think we are still adapting to that change.[9]

New Solutions to Old Problems

The third implication is that new technologies are enabling new solutions to old problems, which means that foreign ministries will have to broaden their range of traditional partners. The most obvious example of this is taking place right now in the Middle East and North Africa, where Twitter and Facebook are helping to reshape the political landscape in a way no one could have imagined.

Governments interested in spurring these democratic revolutions have had to push for internet and phone networks to remain active. In some cases, like the Iranian uprising in 2009, the US State Department asked Twitter to delay a scheduled network upgrade so protestors could keep using the service to organise themselves.[10]

Now that the world has somewhere near five billion mobile phones, a rapidly increasing proportion of which are connected online, foreign ministries have new opportunities for solving problems, particularly those to which solutions have so far been elusive. Many of these opportunities are hard to predict, but crowd sourcing is a good example.

Following the recent earthquake and tsunami in Japan, the Google-developed Person Finder[11] was used to trace more than 300,000 people whose names had been entered into a public database of missing and found people. This project was developed in collaboration with the US State Department.

Crowd sourcing has also been used in Mexico to develop a free short code to allow people to report crime anonymously[12]; it has been used to report electoral violence in India;[13] and is being used by Google to monitor flu outbreaks.[14]

Another example in the public diplomacy realm came after the earthquake in Haiti, where a US telecommunications entrepreneur set up a short code for the State Department allowing US citizens to text a number on their phones which would donate $US10 to the relief effort. The code was set up within 48 hours of the disaster and the State Department raised some $US35 million. It has been used in several subsequent natural disasters.

Given that most government departments won't have the expertise to properly harness these tools, it will probably result in many more partnerships between foreign ministries and external partners.

E-diplomacy is not a boutique extra for foreign ministries and increasingly will be central to how they operate in the 21st century. Digital platforms will require cultural change, but they also promise a wide range of benefits, whether that is taking a much more active role in managing their public diplomacy messages or engaging audiences that were previously out of reach. For DFAT, it is high time to act.

[1] Eric Schmidt and Jared Cohen at the Council on Foreign Relations, 3 November 2010, available online: http://www.youtube.com/watch?v=eJAMD5p5tQo (accessed 29 March 2011).

[2] Ibid.

[3] Mathew Ingram, 'Mary Meeker: Mobile internet will soon overtake fixed internet', GigaOm, 12 April 2010, available online: http://gigaom.com/2010/04/12/mary-meeker-mobile-internet-will-soon-overtake-fixed-internet/ (accessed 29 March 2011).

[4] International Telecommunication Union, Internet users, available online: http://www.itu.int/ITU-D/ict/statistics/ (accessed 29 March 2011).

[5] Matthew Lee, 'US diplomacy embracing Twitter amid global crises', *Washington Post*, 24 January 2011.

[6] US Embassy Jakarta, Indonesia, Facebook: http://www.facebook.com/jakarta.usembassy

[7] US Embassy Jakarta, 'Mission Indonesia funding request to amplify social media effort in time for March POTUS visit', 12 February 2010, available online: http://www.dazzlepod.com/cable/10JAKARTA186/1/ (accessed 29 March 2011).

[8] Fergus Hanson, *A Digital DFAT: Joining the 21st Century*, Lowy Institute for International Policy, November 2010, available online: http://www.lowyinstitute.org/Publication.asp?pid=1432 (accessed 29 March 2011).

[9] George Megalogenis, *Trivial Pursuit: Leadership and the end of the reform era*, Quarterly Essay No. 40, 2010, p. 73.

[10] Lev Grossman, , 'Iran Protests: Twitter, the Medium of the Movement', *TIME* , 17 June 2009, available online: http://www.time.com/time/world/article/0,8599,1905125,00.html (accessed 29 March 2011).

[11] http://japan.person-finder.appspot.com/?lang=en

[12] See Hanson, op. cit., pp. 12-13.

[13] Ushahidi, 'Vote Report India launches', http://blog.ushahidi.com/index.php/2009/04/07/vote-report-india-launches/

[14] Google, http://www.google.org/flutrends/

New Media and Democracy: the Middle East as Testing-Ground

Dr Anthony Billingsley[*]

In the light of the great expectations held for new media in the promotion of democratic change, the Middle East and North Africa represents, in many respects, a prime case study of the actual and potential impact of new information and communications technology. The recent dramatic challenges to long-established rulers across almost every country of the region would appear to bear out some of the hopes of the supporters of new media. In short, new media are seen as encouraging a greater interest and participation in the political process among people who have been largely disillusioned by their political system. This is, in part, because the new technologies allow for the flow of information and ideas allowing for an interaction that is immediate, simple and even personal.[1] Such technologies have acquired an almost subversive capacity to challenge the extensive control of societies in the region by ruling elites and may, over the longer term, force political activity into a new model.

In a speech in January 2010, US Secretary of State Hillary Clinton spoke about the way in which internet-related technologies promote the dissemination of information and how this can help citizens to hold their governments accountable and to organise movements for freedom.[2] At the time the Secretary of State was speaking generally but her remarks have particular relevance in the light of what has been happening across the Middle East and North Africa. The region is dominated by authoritarian states, which are intolerant of dissent and which enforce

[*] Dr Anthony Billingsley is a Lecturer in the School of Social Sciences and International Studies at the University of New South Wales.

their control over society through intensive and intrusive censorship and the manipulation of education and information. Traditional forms of media have served as vital mouthpieces of official policy; while they lack credibility among the people of the area, they have until relatively recently been among the only sources of information available to populations in the region. For the democratic process to be take root in the region, this domination of information by the state has to be by-passed. New forms of media are seen to be the means to this end.

In the Middle East and North Africa people have had extensive access to many forms of new media for some time. And they have learnt to exploit the decentralised nature of the technologies to facilitate the wide distribution of information to the population. In so doing, new media appear to have encouraged people to question government behaviour and to organise demonstrations of their dissent in ways that have made government counter-measures difficult. The extraordinary unrest in Iran following the disputed Presidential elections in 2009 – and the refusal of the Iranian people to accept the claims and demands of their government – is said to be evidence of the huge and irresistible force of new media in the hands of a determined population. The people of Tehran drew heavily on new media for the cohesion of their resistance and their tenacity in the face of intense government repression. The downfall of the Egyptian dictator, Hosni Mubarak, has been termed the 'Facebook revolution' in the international media. The clear evidence of the role of mobile phones and other media in energising and sustaining the demonstrators in Cairo's Tahrir Square – perhaps the Middle Eastern equivalent of the phenomenon of 'swarming' – would seem to support a decisive role for new media in the promotion of democracy in that country. The unfolding of events in countries across the region would seem to support Secretary Clinton's view that new media can contribute to the application of pressure on governments to be open and accountable.

When one looks more closely at the events in Tehran, Cairo and elsewhere across the region, however, it is more difficult to attribute immediate gains to the new forms of media. There are important questions to ask regarding the extent to which new communication technologies have made a real contribution to the goal of political change and whether this contribution is significantly different from and greater than more traditional approaches. Are they as significant in their impact on political life as the invention of the printing press and radio? Do they really represent what Larry Diamond has termed 'liberation technology'?[3] The answers to these questions are far from clear.

In the case of Egypt, for example, mobile phones and other new media were initially in evidence until the government began to shut the networks on which they rely. In response, people began to fall back on more traditional word-of-mouth. Given the high proportion of the Egyptian population which lives in relative proximity to Cairo, word-of-mouth appears to have been very effective in attracting the masses of people who joined together in Tahrir Square and in coordinating the response to the provocations of the government. Citizens of non-democratic countries have developed impressive ways of communicating and organising politically both despite and because of the pressure of government suppression. This has been evident in unrest that has periodically broken out across the countries of the region, such as the uprising in Syria in 1982 when much of the city of Hama rose against the government of Hafez al-Assad.

In assessing the contribution of new media, it is helpful to highlight two dimensions of the role of new media in political change. The first relates to the short-term impact of these media, as typified by the events in the Middle East and North Africa over the past month or so. The second relates the longer-term impact of new media on attitudes towards governance and authority. It is in this second area where new media may make a greater contribution in building a consensus that rejects authoritarian regimes.

Looking at the issue of short-term impact, much of the information that was circulated through the new media was useful in assisting the cause of dissent. It would also seem clear, however, that much of the information that did the rounds of the crowds across the region was not accurate or useful. In the early days of the Libyan revolt, for example, reports circulated widely that Colonel Qaddafi had fled to Venezuela. These reports enjoyed credence in the new media even though they were without any basis in fact, and were only halted by Colonel Qaddafi's appearance on television. This highlights a feature of new media, which is to enable the dissemination of information widely and quickly but without subjecting that information or opinion to any level of scrutiny or reflection. In such an instance, these media do not add any substance to the debate about the sorts of things people want – nor do they provide focus to help people to make sense of the information that they are receiving. If anything, there is a risk that they trivialise issues and the processes involved and this is a particular problem if new media are seen as having a role in the promotion of democracy. The promotion of such a complex and controversial issue cannot be introduced, promoted and adopted by means of what are effectively short advertisements, which is how some new media such as Twitter operate. Diamond refers to this as cacophony over pluralism and "an 'echo chamber' of the ideologically like-minded".[4]

Among the different new media technologies, blogs most closely approximates the approach of traditional media in providing the opportunity for a degree of reasoned debate. A quick trawl through blogs in Australia and other countries will bring to light many thoughtful, informed and beneficial contributions to debate on a range of issues. The same process, however, will also uncover many splenetic, ill-informed sites that feed people's prejudices, fears and ignorance without a sense of responsibility for any repercussions. Blogs have served an important role in the unrest in the Middle East but again there have been problems of balance and accuracy in some.

Secretary Clinton, in her speech noted above, commented that new information and communication technologies are a double-edged sword. She was referring specifically to the ability of groups like Al Qa'ida to promote their ideologies through new media. In addition there is a related but different problem to consider. People can certainly try to use SMS to promote democracy in a society and Al Qa'ida can use the technology to spread its world view, but governments are equally capable of using those same technologies to promote their own perspectives. So, Colonel Qaddafi reportedly sent SMS messages to people in Benghazi warning them that he was about to attack their city soon with the intention of spreading panic among the population. (Probably an unnecessary step as people there already had cause for alarm.) More fundamentally, governments appear to have adapted quickly to the challenge posed by new technology by developing sophisticated means of filtering sites and material and effectively controlling the new networks. Given the reliance of new media on the telephone system – which in most non-democratic countries is likely to be state-owned and run and highly centralised – more modern means of communication would appear to be just as vulnerable to state censorship as any other means of communication.[5]

Looking at some of the dramatic events playing themselves out in the Middle East and North Africa, for which new media are being given credit, it is by no means certain that their short-term impact has been of any lasting significance. In Iran, for example, the regime increasingly applied the force at its disposal in response to the demonstrations and blocked the population's ability to communicate through new media. Moreover, the flurry of SMS, Facebook and other activity tended to be conducted in something of an ideological vacuum. There was no long term debate to help people clarify their hopes and goals. In Egypt, some people clearly had a form of democratic revolution in mind. Others, perhaps the majority, simply wanted the hated dictator to go.

Moreover, the role of more conventional media has remained important throughout the crises in the Middle East and North Africa. The Qatari-based television channel Al Jazeera has been perhaps the single most important medium for the distribution of useful and influential information about the crises. Even in the many countries where governments have attempted to block access to Al Jazeera, people have managed to work around government controls. While susceptible to the control of its host government, Al Jazeera has managed to exert an extensive influence throughout the region as a whole. The way in which it has opened people's eyes to the problems and hypocrisies of the region over the years since its establishment has arguably contributed more to recent developments than other forms of media. Al Jazeera has provided information that is trusted in a way that government-controlled media organisations could never be. This has enabled the network to provide a necessary filter of information and a level of organisation of news that gives it meaning to its readers.

In the longer-term, however, it would be a mistake to dismiss the impact on autocratic societies of new media such as Facebook and Twitter. It may be that these forms of media, like the more traditional forms, are vulnerable to the power of the state in a direct confrontation such as we have seen in Bahrain. But there is another element to what is happening in the Middle East and North Africa. While it is still early days in the revolutions challenging established regimes across the region, these 'subversive' means of communication, for all their faults and their trivialisation of events, appear to be undermining the basis on which oppressive regimes have operated for years.

In their day, the printing press, the telegraph, radio and television revolutionised the way in which information was distributed and this deeply influenced political behaviour. Their effects also tended to be felt along generational lines, with older generations holding to the forms of media with which they were comfortable and younger generations accepting more enthusiastically the opportunities offered by the new technologies. We have perhaps seen a similar process at work in the lead up to the public displays of defiance of authority in the Middle East and North Africa.

Young people in the region, where about 60% of the population is under 30 years of age, have been using new media long before the various outbreaks of unrest throughout the region. In the course of this activity they have been able to reconsider the established rules of society that have furthered autocratic control. Strict controls on the freedom of movement of unmarried women, for example, could be bypassed through the digital world without directly challenging parental authority. Young people have been able to communicate and to network in ways that have encouraged them to realise that other ways of ordering society might be possible. New media also provide individuals the opportunity to join large numbers of their peers to analyse and criticise the information provided to them by their governments and to realise that they are not alone in their disillusionment. This process has been happening under the noses of those in power.

Of course, there is nothing in the new technologies to indicate that some form of democratic governance will be the result of the changing attitudes of the younger generation throughout the Middle East and North Africa. Often (to their dismay) younger generations display the influences of their parents' opinions and values. It can safely be assumed that Gamal Mubarak, who was understood to be slated by his father to take over the Egyptian presidency, would share many of his father's views on the way in which the Egyptian state should be run. Gamal would, however, probably also have shared the same enthusiasm for the internet and other modern forms of communication with people of his generation.

Moreover, the demands of the people of the region are by no means clear. As suggested above, demonstrators in Egypt, Tunisia and Libya were united in their desire to see the dictator go. The picture of what is to come next, however, is less than clear. Some protesters evidently want some form of democracy. Others probably are concerned to maintain a degree of stability in society and the economy and only want sufficient change to make the political system more accessible, more responsive to their concerns and less corrupt.

Nevertheless, the effects of the developments we have been witnessing are far-reaching. In the short-term, the state continues to exercise power through its monopoly of the use of force and its ability to inhibit the use of new media. This means that there will still be constraints on the impact of new media. It could mean, however, that the next generation of leaders of society will no longer accept the traditional ways of ordering society. Instead, they may reflect a consensus that has been developing over some time, thanks in large part to the new media, which rejects traditional forms of control and accepted understandings of society's priorities. This consensus may make the existing authoritarian regimes of the Middle East and North Africa unsustainable.

The impact of new media in the Middle East and North Africa has been dramatic and far reaching. It has empowered people, especially the younger generations, to question the way in which their societies have been ordered over the past 30 to 40 years. It has set in train a process that may lead over time to widespread rejection of the authoritarian political process that has dominated the region for generations and may lead to more responsive political structures in the future.

[1] Steven Barnett, 'New Media, Old Problems: New Technology and the Political Process', European Journal of Communication, Vol. 12, No. 2, June 1997, pp. 193-218.

[2] Secretary of State Hillary Rodham Clinton, Remarks on Internet Freedom, 21 January 2010, available: http://www.america.gov/st/texttrans-english/2010/January/20100121142618eaifas0.6585352.html (accessed 20 March 2011).

[3] Larry Diamond, 'Liberation Technology', *Journal of Democracy,* Vol. 21, No.3, July 2010, pp. 69-83.

[4] Diamond, ibid., p. 80.

[5] See for example, Barnett, op cit.

The Dark Side of the Net:
Past, Present and Future of the Cyberthreat Story

Dr Myriam Dunn Cavelty*

Information has always been a significant aspect of power, diplomacy and armed conflict. Recently, however, the importance of information as a factor in political matters has spectacularly increased due to the triumphant proliferation of information and communication technology (ICT) into all aspects of life. The ability to master the generation, management, use and also manipulation of information with the help of these technologies has become a much-desired power resource in international relations.

But where there is opportunity, there is threat. The cyberthreat story is a story initially shaped and told by American security professionals. However, the story has spread as if the expanding computer networks carried their own (in-)security logic with them across the globe. Existing variations in the story are mere variations of detail, not differences about the actual substance.

This (in-)security logic deserves special attention. First, it provides the backdrop for today's cyber-plot. Understanding it helps to understand the fabric of current issues and fears. Second, the threat story also defines the possibilities and logics of protection, which are a direct result of how the past, present, and also the future of the cyberthreat is seen.

From Government Networks to Critical Infrastructure

The merger of telecommunications with computers in the late 1970s and 1980s – the basis of the current information revolution – marks the

* Dr Myriam Dunn Cavelty is a Fellow at the Stiftung Neue Verantwortung, Berlin and Head of the New Risk Research Unit at the Center for Security Studies, ETH Zurich.

beginning of the cyberthreat story. The introduction of the personal computer created a rise in tech-savvy users, who became theoretically able to make ‘bad’ use of emerging computer networks and actually did so in many cases. At the time, the amount of attention given to computer and communications security issues in politics grew incrementally in response to highly publicized events such as politically motivated attacks, computer viruses, espionage, data theft and penetration of networked computer systems for criminal purposes.

At first, the overarching concern was with government information systems – or rather the classified information residing in them. With the growth and spreading of computer networks into more and more aspects of everyday life, however, the debate changed noticeably. In the late 1980s and especially in the 1990s documents started to appear that made a clear link between cyberthreats and so-called critical infrastructure: assets deemed critical because their incapacitation or destruction could have a debilitating impact on the national security and/or economic and social welfare of the entire nation. Rather than limited proprietary networks, the object of protection began thus to encompass the whole of society – or rather, its way of life provided by the uninterrupted sub-structure of technology. [1]

This threat perception was decisively influenced by the larger strategic context that emerged after the Cold War, when the notion of asymmetric vulnerabilities, epitomized by the multiplication of malicious actors (both state and non-state) and their increasing capability to do harm, started to play a key role. Due to difficulties in locating and identifying enemies, parts of the focus of security policies shifted away from actors, capabilities and motivations towards general vulnerabilities of entire societies. The US as the only remaining superpower was seen as being predestined to become the target of asymmetric warfare. Widespread fear took root in the strategic community that those likely to fail against the US war machine might instead plan to bring the US to its knees by striking against vital points at home: namely, critical infrastructure.[2]

An Overwhelming Threat?

The concept of critical infrastructure includes sectors such as information and telecommunications, financial services, energy and utilities, transport and distribution. It also includes a list of additional elements that vary across countries and over time.[3] Most of these sectors rely on a spectrum of software-based control systems for their smooth, reliable and continuous operation. The information infrastructure serves as an intermediary between physical assets and physical infrastructure. Bridged and interlinked by information pathways, critical infrastructure systems thus spread over more and more territory. An increasing number of networks, nodes and growing interdependence in and among these systems increase their complexity, to the point where it becomes intellectually overwhelming.

There are two ways that an image of threat is formed. First, an inward-looking narrative equates complexity with vulnerability. The very connectedness of infrastructure systems is what poses dangers, because perturbations within them can cascade into major disasters with immense speed and beyond our control. Second, an outward-looking narrative sees the increasing willingness of malicious actors to exploit vulnerabilities without hesitation or restraint. Because critical infrastructure systems combine symbolic and instrumental values, attacking them becomes integral to a modern logic of destruction that seeks maximum impact. In other words, cyberspace becomes a force-multiplier by combining the risks to cyberspace with the possibility of risks through cyberspace.[4] It reformulates space into something no longer embedded into place or presence. Laws of nature, especially physics, do not apply into this non-space/place,; there are no linear distances, no bodies, no physical co-presences. The 'enemy' becomes a faceless and remote entity, a great unknown that is almost impossible to track.

This results in two significant and very powerful characteristics of the threat representation. First, the protective capacity of space is obliterated; there is no place that is safe from an attack or from catastrophic breakdown in general. The threat becomes one with the network; it *is* the network. Second, the threat becomes quasi-universal because it is now everywhere, creating a sense of "imminent but inexact catastrophe, lurking just beneath the surface of normal, technologised [...] everyday life".[5] This creates a distressing limbo state of 'not-safe-but-waiting-for-destruction/disaster';:a disaster which is implicitly construed as inevitable.

A New Chapter: The Stuxnetification of the Story

But despite of this all-embracing potential for major disaster, the actual factual reality of cyberthreats to date looks far less stark. In the entire history of computer networks, there have only been very few examples of severe attacks that had the potential to or did disrupt the activities of a nation state in a major way. There are even fewer examples of cyberattacks that resulted in physical violence against persons or property. Though it is the norm today that every political tension or conflict is accompanied by heightened activity in cyberspace, the huge majority of cyberattacks are low level and cause inconvenience rather than serious or long-term disruptions.

Stuxnet, however, was not low level. And though its exact effects remain a mystery, it has changed the cyberthreat story once and for all.

Stories and speculations about the worm, its origins and its intent exist by the thousands by now.[6] Well-written or less so, they all contain bits and pieces of a puzzle that is inherently unsolvable but highly newsworthy. The gist of it is this: Stuxnet is a computer worm that seems to have been written to specifically attack Supervisory Control And Data Acquisition (SCADA) systems used to control and monitor industrial processes. It behaves differently from the usual criminal malware: it does not steal information, it does not herd infected computers into so-called botnets in order to launch criminal attacks and it does not spread indiscriminately. Instead Stuxnet performs sabotage; in particular, there is evidence that it may have been targeted specifically at the Iranian nuclear program. Stuxnet is a very complex programme: according to experts, writing it not only requires in-depth computer geek skills but also knowledge of industrial processes. Stuxnet was also very expensive to create: estimates by Symantec conclude that it may have taken 8 to 10 people six months to complete.

The combination of all these factors can lead to the conclusion that only one or several nation states would have the capability and interest to produce and release Stuxnet. If so, the ‘digital first strike’ has occurred – bringing cyberwar from the realm of the possible into the hard reality of a strategic world, which could soon see the unchecked use of information weapons in military-like aggressions.

Given such train of thought it is little surprising that the discovery of Stuxnet has scared government officials out of their wits. All over the world, governments are currently releasing or updating cybersecurity strategies and setting up new organisation units for cyberdefense. While such reactions are probably having an overall positive effect on the level of cybersecurity worldwide, one cannot help but wonder whether a little more level-headedness would not be beneficial for everybody in the long run.

First, it should not be forgotten that who has really programmed and released the worm remains unknown, even though the usual ‘cui bono’ logic pointing either to the US or Israel is convincing. ‘Attribution’, that is the ability to attribute an attack to a particular person or party, is one of the bigger problems the cybercommunity faces. In the case of Stuxnet, there is only one party that really knows who is behind it and what the target really was: those involved in programming and releasing the worm. Even intelligence information on the cyber capabilities of other state and non-state actors is largely based on sophisticated ‘guesstimation, since it is simply impossible to know who has access to cyberweapons (which is nothing more than a 'sexy word for software) without scanning all computers and storage devices owned by them, including all classified systems.

Second, regardless of who is or is not behind it, Stuxnet is not about war. Nobody denies that modern societies are connected through dense networks and depend on these networks for proper functioning. Theoretically, these societies are thus vulnerable. But the hacking of websites is no cyberwar. Espionage on the Internet or the theft of industrial secrets with the help of computers is no cyberwar. Electronic warfare is no cyberwar. The spreading of half-truths or false information is no cyberwar. Not even sabotaging an industrial plant with sophisticated malware is cyberwar. Though dubbing these activities cyber 'war' might be an often thoughtless and really rather harmless act by most, the use of the word "war" by state officials in the international arena bears the inherent danger of creating an atmosphere of insecurity and tension.

Amidst all the brouhaha, one crucial lesson seems to have been forgotten by nearly everyone: in security and defence matters, careful threat assessments need to be made. And such assessments necessarily demand more than just navel-gazing and vulnerability spotting. Though many aspects are new, others are not; the logic of strategy remains unchanged in principle. Even if the most extreme case is assumed – that the majority of states in this world have developed effective and powerful cyberweapons – the mere existence and availability of such capabilities would still not automatically mean that they would be used. In fact, it has been convincingly shown that a 'pure' (or strategic) cyberwar is very unlikely to ever occur, with attacks on computer systems more likely to be used in conjunction with other, physical forms of attack.[7] For many democratic states, the risk of war has moved far to the background. The risk of a cyberattack of the severest proportions should be treated the same.

Third, rather than just assuming the worst, the question that must be asked is: who has the interest and the capability to attack us and why? If thought through carefully, Stuxnet-like weapons need not worry decision-makers much either. Unlike a nuclear weapon, a cyberweapon cannot be stored in a silo for decades. To obtain a specific and controllable effect, the system one aims to attack must be known in detail and the ‘weapon’ needs to be tailored to a specific vulnerability – and to nothing else. There is a high possibility that this vulnerability is fixed before programming is complete, especially when the production time is long. There is also no guarantee that the weapon will work if released: the more complex the software, the more likely it is that it contains its own flaws. Therefore, though the cost of such a weapon is nowhere near the cost of a physical bomb, the risk of failure is very high. What appears to be a cheap solution for unbloody war might in fact turn out to be far too expensive for what it can deliver.

The development and release of such software makes sense in one particular case, however, given a high level of tension between states as a precondition: when it comes to the sabotage of weapons programs or other high profile or high-risk facilities. Then only, the advantages of a stand-alone cyber-attack may come to full fruition: if the malware were to run error-free, undetected interference would be possible, which would drastically reduce the risk of armed escalation. If something went (technically) wrong and the malware was discovered (as is the case with Stuxnet), difficulties attributing authorship would still make retaliatory action unlikely.

Fourth, though Stuxnet has indeed changed the cyberthreat story in profound ways, it has actually *not* changed its essence or its substance, but only its reach, by turning the issue from an issue of the few to an issue of the many. In fact, experts have been expecting a major occurrence in cyberspace for a long time; seen this way, Stuxnet is less of a surprise and more of a confirmation. Likewise, the protection of critical infrastructures has been on the agenda for more than a decade. Much of what needs to be done is well known and Stuxnet confirms that, too. Rather than expecting inevitable cyberdoom, the future of the cyberthreat can be shaped by human choices in the present.

Mitigation through Cooperation

Over the years, five types of responses have become common in critical infrastructure protection (CIP) practices worldwide.[8] Rather than trying to know and anticipate specific threats, response strategies are geared towards mitigating the risk of all contingencies by reducing vulnerabilities; this is mainly achieved through cooperation.

First, an increase of public-private collaboration to enable a better exchange of information is pursued. A functioning partnership between the state and the corporate sector is essential: due to the liberalization of many public sectors since the 1980s, a large part of the critical infrastructure is privately administered today. Therefore, the private sector has a key role in defining and implementing protective policies. Governments will want operators to take responsibility for the implementation of protection measures that are in accordance with the parameters or frameworks set by public authorities.

A second measure is to better coordinate a more integrated approach on the domestic front. Often, there are too many governmental agencies involved in CIP and/or cybersecurity matters. In consequence, it has often been impossible to attribute clear responsibilities, which hinders effective response. In a move to centralize CIP, many states have developed new structures or offices that are responsible for overseeing the activities of all the agencies that deal with CIP-related issues.

Third, CIP can only work if the wider society becomes more aware of public vulnerability and the importance of public participation in building CIP policies. Therefore, public awareness campaigns are required. In addition, there is also a need for enhanced support of cybereducation from elementary schools to colleges and universities, training of a capable and technologically advanced workforce and research in the rapidly evolving field of cyberspace. Together these should lead to better protection.

Fourth, the efficacy of national efforts remains limited: the vulnerability of modern societies has global origins and implications. Therefore, despite the fact that international cooperation is in many ways already taking place, expanded and more efficient cooperation is needed, particularly when it comes to international legal cooperation. The avenues currently available for arms control in this arena are primarily information exchange and norm-building; by contrast, attempts to prohibit the means of cyberwar altogether or restricting the availability of cyber weapons are likely to fail.

Fifth, and more recently, a shift away from the concept of protection towards the concept of 'resilience' can be observed. Though the two concepts overlap often, infrastructure protection aims to prevent or reduce the effect of adverse events, while infrastructure resilience reduces the magnitude, impact or duration of a disruption.

The Logic of Security in the Cyber-Domain

Resilience is not a new concept, of course, but its current rise indicates a significant and crucial shift in thinking. While protective (and defensive) measures aim to prevent disruptions from happening, resilience accepts that certain disruptions are inevitable. If resilience is a core concept, security does not refer to the absence of danger but rather the ability of a system quickly and efficiently to reorganise to rebound from a potentially catastrophic event.

Such thinking is absolutely necessary if cyberthreat issues are to be tackled successfully. The problem that needs to be overcome is that two different types of security logics are clashing when cybersecurity is framed as national security issue. In national security, security is a binary concept: either one is secure or one is insecure. By contrast, computer security or information assurance is concerned with analysing the risk to information networks of all sorts and then mitigating the identified risks by technical (and occasionally organisational) means. Risk is a probabilistic concept aimed at managing an ongoing process, and is by definition linked to the notion of insecurity. As every systems administrator knows, his or her goal is not to eliminate risks, but to manage them in the most cost-effective way. Information networks, therefore, can never be 'secure' in the national security sense. In fact, the opposite is true: cyberincidents are deemed to happen under the risk logic, because they simply cannot be avoided.

Given the nature and scope of the cyberthreat, governments must think of ways to communicate the fact that 'cybersecurity' is a misnomer and think of recipes for higher fault tolerance. If governments continue to build up an infallibility paradigm a major public relations disaster (or worse) is bound to occur. Governments must also be ready to admit that their role in cybersecurity can only be a very limited one, even though they consider cyberthreats to be a major national security threat. The challenge facing governments is to maintain their role in protecting critical infrastructure where necessary, while determining how best to encourage market forces to improve the resilience of companies and sectors, and to ensure that cooperation among private actors operates smoothly even without constant oversight.[9]

The yin and yang of the cyberworld teaches us there cannot be good without bad. To continue reaping the benefits of the cyberage, it is necessary to learn how to live with insecurity in pragmatic ways.

[1] Myriam Dunn Cavelty, 'Cyber-Security', in: Peter Burgess, ed., *The Routledge Handbook of New Security Studies* (London: Routledge, 2010), pp. 154-62.

[2] Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (London: Routledge, 2008).

[3] Elgin Brunner and Manuel Suter, *International CIIP Handbook 2008/2009*, Center for Security Studies, Zurich. Available online: http://www.crn.ethz.ch/publications/crn_team/detail.cfm?id=90663 (accessed 29 March 2011).

[4] Robert Deibert and Rafal Rohozinski, 'Risking Security: Policies and Paradoxes of Cyberspace Security', *International Political Sociology*, 2010, vol. 4, pp. 15–32.

[5] Stephen Graham, 'Cities and the "War on Terror"', *International Journal of Urban and Regional Research*, 2006, Vol. 30, No. 2, pp. 255–276; quoted p. 258.

[6] Two prominent examples are: Mark Clayton, 21 September 2010, *The Christian Monitor*, available online:

www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant (accessed 29 March 2011); Michael Joseph Gross, April 2011, 'A Declaration of Cyber-War', *Vanity Fair*, available online: www.vanityfair.com/culture/features/2011/04/stuxnet-201104 (accessed 29 March 2011).

[7] Peter Sommer and Ian Sommer, 'Reducing Systemic Cybersecurity Risk', OECD/IFP Project on Future Global Shocks, 2011, available online: www.oecd.org/dataoecd/3/42/46894657.pdf (accessed 29 March 2011).

[8] Elgin Brunner, Anna Michalkova, Manuel Suter and Myriam Dunn Cavelty, Focal Report 3 - Critical Infrastructure Protection: Cybersecurity – Recent Strategies and Policies: An Analysis, 2009, Center for Security Studies, Zürich. Available online: www.crn.ethz.ch/publications/crn_team/detail.cfm?lng=en&id=108735 (accessed 29 March 2011).

[9] Myriam Dunn Cavelty and Manuel Suter, 'Public-Private Partnerships are no Silver Bulled: An Expanded Governance Model For Critical Infrastructure Protection', *International Journal of Critical Infrastructure Protection*, 2009, Vol. 2, No. 4, pp. 179-187.

Biographies of Contributors

Anthony Billingsley

Dr Anthony Billingsley is a Lecturer in the School of Social Sciences and International Studies at the University of New South Wales. He teaches courses in international affairs, international law and on the Middle East. His specialist interests include political succession in the Arab world, the role of constitutions and law in the region and the politics of the Gulf, Syria and Egypt. His most recent books are *International Law and the Use of Force* (co-authored with Shirley Scott and Christopher Michaelson) and *Political Succession in the Arab World: Constitutions, Family Loyalties and Islam*.

Alison Broinowski

Dr Alison Broinowski, formerly an Australian diplomat, has written and edited eleven books about the interface between Australia and Asia and Australia's role in world affairs. She is a visiting Fellow at ANU and a Senior Research Fellow at the University of Wollongong, where she has just completed an ARC-funded project on Asian Australian fiction, the results of which appear as a set of ten papers in *Antipodes* in June 2011. Her most recent book, *Allied and Addicted* (Scribe, 2007) challenges the value of the Australian-American alliance. Her last overseas assignment was in the Australian Mission to the UN in 1989-90, and in 2005 she co-published with James Wilkinson *The Third Try: Can the UN Work?*

Myriam Dunn Cavelty

Dr Myriam Dunn Cavelty is a Fellow at the Stiftung Neue Verantwortung, Berlin and Head of the New Risk Research Unit at the Center for Security Studies, ETH Zurich. She publishes regularly in international journals and has authored and edited several books on information age security issues such as *Cyber-Security and Threat*

Politics: US Efforts to Secure the Information Age (Routledge 2008); *Securing the Homeland: Critical Infrastructure, Risk, and (In)Security* (Routledge 2008); and *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace* (Ashgate 2007). In addition to her teaching, research and publishing activities, she advises governments, international institutions and companies in the areas of cyber security, cyber warfare, critical infrastructure protection, risk analysis and strategic foresight. As an internationally renowned cyber expert she is a frequent speaker at professional conferences.

Fergus Hanson

Mr Fergus Hanson is the Director of Polling and a Research Fellow at the Lowy Institute. He has a Masters in International Law from the University of Sydney. Fergus worked for the Department of Foreign Affairs and Trade (DFAT) from 2004 to 2007. From 2005 to 2007 he served at the Australian Embassy in The Hague where he was responsible for Australia's relations with five international legal organisations and domestic political issues. Fergus was a visiting Vasey Fellow at the Center for Strategic and International Studies, Pacific Forum from November 2010 to January 2011. He was awarded a 2011 Professional Fulbright scholarship to pursue further research on e-diplomacy and the use of opinion polling by foreign ministries.