Omer Rana (Cybersecurity)
School of Computer Science & Informatics, Cardiff University
ranaof@cardiff.ac.uk
Twitter: @omerfrana

The NATO "Cyber Security Framework Manual" (2012) from NATO Cooperative Cyberdefence CoE [1] -- and reports from organisations such as ENISA (European Network and Information Security Agency) [2] discuss the differences in National CyberSecurity Strategies (NSS) across NATO states. It is useful to see the change in emphasis on what constitutes "cyberspace" across different nation states. Some countries take a broad view of cyberspace that includes infrastructures (such as control systems in critical infrastructures) and others take a much narrower view of cyberspace, equating it more closely to the internet. To illustrate, the United States is at one end of the spectrum with a broad definition of cyberspace, even implicitly acknowledging the importance of social networks. Similarly, the UK NCSS emphasises the need to make cyberspace a safe place for both citizens and businesses. In the Dutch NCSS, cyberspace is likewise defined broadly, including chip cards and in-car systems. On the other side of the spectrum, countries like Australia, Canada, Germany, New Zealand and Spain place an emphasis on the internet and internet connected information technologies.

Nations are constantly facing the twin tensions of how to expedite the economic benefits of ICT and the internet economy while, at the same time, protecting intellectual property and privacy (data protection), securing critical infrastructure, and providing for defence of the homeland. In some countries the internet contributes up to 8% of gross domestic product (GDP), with estimates of 60% of the world population being on-line by 2020. Member countries of both the European Union (EU) and the G20 have established goals to increase the internet's contribution to GDP. This cyber environment's value and potential is nurtured by private and public sector investments in high-speed broadband networks and affordable mobile internet access. Three issues are central to the national security debate in this context: how does the government assure the availability of essential services; provide for the protection of intellectual property; and maintain citizen confidence (and safety) when participating in the internet economy? Nations are struggling with finding the appropriate mix of policy interventions and market levers to address these issues.

An issue for future consideration is how existing National CyberSecurity Strategy (NCSS for short) can cope with rapidly changing threat dynamics. In other words, with no formal review mechanism in place, many NCSS may become irrelevant or unable to provide guidance when facing a new type of cyber challenge. Only a few countries have released more than one NCSS. A key question in this context remains on how to overcome the risk of a mismatch between technology development and security policy.

To keep this contribution focused, I shall discuss one particular recent IT innovation – the use of Cloud computing. Citizens, businesses and government departments have started to make use of Cloud environments for a variety of reason – ease of access, low cost of access, ease of scaling the infrastructure with demand, energy savings, consolidation etc. Even organisations such as Universities who traditionally managed their own IT infrastructures are now outsourcing services to Cloud providers – such as Google and Microsoft. Cardiff University, for instance, uses Microsoft Office 365 to offer email services to employees. How much are customers aware of how companies such as Microsoft and Google make use of their data?

There has also been a significant rise in the use of Cloud systems by citizens (in some instance, without them realising this!) – for instance, by extending mobile devices to directly make use of Cloud-based services. The emerging area of "mobile offloading" enables mobile devices (smart phones, tablets and in the future cars) to run services on Cloud systems to enable better use of battery power and utilize more complex capability that is hard to host on a mobile environment. Car-based services will become more dominant in the future, as more complex information infrastructures are embedded within vehicles.

There is, off course, also significant interest in NATO about the use of Cloud computing – and how the NATO business model, fairly distributed and involving global operations, can be supported through a Cloud environment. At the NATO C4ISR Industry conference (March 2014) this year [4], Cloud computing was identified for increasing availability and consolidation of NATO services (reducing costs, better sustainability). One area of interest was command-and-control capability. A key question considered was how public vs. private Clouds could be used to host and support NATO operations post-Afghanistan, and how NATO members would respond if critical applications in the future were available in a Cloud-only model. As each nation has its own computer network and needs to support interoperability, understanding how a standards based approach could be followed was also outlined. Also seen as a requirement as part of the NATO C4ISR and the NATO Communications and Information (NCI) Agency.

Two questions t o consider:

With Cloud computing, what role should government play – alongside commercial providers – as a regulator, an enabler/facilitator, as a user (or all over the above)?

With significant dominance of Cloud computing – and its associated reliance on broadband internet – should NCSS also reflect use/abuse of such systems? Are NATO states really geared up to address this?

I finish with security challenges in three areas: technical, social and organisational in the context of Cloud computing:

Technical:
Cloud security issues:

- The boundary of an organisation can be extended through Bring-your-own-Cloud technologies (extending organisational boundaries through public Cloud offerings –e.g use of DropBox and variants, use of Google-based services, etc) – limiting the security control that an organisation can have over these.
- The volume of data held in Cloud systems and transferred between Cloud systems makes auditability and verifiability almost impossible. As more and more data becomes on-line and people utilise this to inform their decision making – ensuring that this data is actually "fit for purpose" also becomes a challenge. Tampering of Cloud-hosted data that could be produced by a government department – for instance – could have an impact on its subsequent use. Can we place similar levels of reliance on electronically held data sources as we did previously on printed versions?
- Moving personal data to Cloud systems – raises issues of jurisdiction (where the data is held and who can see the data). Data can be moved between different data centres to enable energy conservation or save on costs by Cloud providers. These migration actions are often not directly exposed to users.

- Many Cloud providers focus on performance issues (latency, response time targets) – very few actually provide support for security in service level agreements they establish with users. The need to support Cloud certification to provide greater degree of trust in such providers is necessary. Very few standard offerings contain security and privacy guarantees, except for basic data protection guarantees, such as whether—and how stored data will be encrypted, what kind of authentication and access control mechanisms are in place, what kind of certificates the provider holds and sometimes also information on what geographic region the data centers are located in.

Organisational

- Many of the security challenges in cloud computing are in part related to the complex provider supply chains in this ecosystem. It is often extremely difficult to determine where data is being stored or processed at any one time. Similarly, unless fully encrypted (during storage and analysis), cloud providers often have to be trusted with data.
- With an emerging "cloud ecosystem" there is now a diffuse "fog" of several cloud providers. For instance, a service provider can adapt and compose several services into one, which is then offered to customers. Similarly, an application that an end-user interacts with is often based on solutions from multiple providers, which in turn is executed on a variety of different physical infrastructures. Numerous combinations exist and more are expected to come. Hence, there will be chains of services and providers involved in the final service delivery. From a security point of view this means that the cloud customer may, sometimes unknowingly, rely on many different parties, hence being subject to multiple points of failures and difficulties in verifying that legislation and internal security policies are being adhered to.
- Rapid change as a result of mergers and acquisitions between companies using or providing services in the cloud, can also result in vaguely defined and/or poorly understood business perimeters.

Social

- There is an increasing use of Clouds to launch cybercrime (no clear definition of what this is amongst the various National Cybersecurity strategies).
- Detection of a "trail of use" that is left behind as criminals make use of Cloud systems is an emerging research area, focusing on "anomaly detection" in Cloud use – which could suggest potential malicious activity taking place within such environments.
- The ease of access to Cloud environments globally also opens up potential for trans-national crime through the use of such infastructures. Are National Security Policies really geared up to address these challenges? The levels of coordination that would be needed across agencies and between government and public-private organisations could lead to interesting challenges that remain unexplored.
- A large majority of cybercrime is unprosecuted and this will become increasingly so as we extend the boundaries our systems – our colleagues at Durham University building a database of cybercrime [5] indicate that since 1991 there have been approximately 300 prosecutions and/or charges relating to cybercrime and under the CMA 1990 law. This is an approximation as certain cases are underreported or do not get to trial. Between 2003 and 2007, for example, there were 61 successful prosecutions under all sections of CMA and in 2012 there were twelve successful prosecutions. Compare this with the actual number of reports from businesses and individuals. As an example of this, Gloucestershire Police reported that between April and December 2013 in their county alone, they had 89 reports from businesses or individuals of 'hacking', 240 reports of online fraud; and 78 reports of online harassment via social. In 2014, Action Fraud listed

350 submitted reports of ‘online shopping and auction’ fraud alone in Gloucestershire over a five month period (February-July 2014). And while it is unclear how many of these reports resulted in a detection or conviction (such as a caution, warning, restorative justice, or custodial sentence), this reported total, during an 8-month period, far exceeds the number of actual convictions over a 23-year period. This, clearly, is worrying!

- There is clearly a social element in all this – to what extent are individuals aware of the potential risk whilst still wanting to trade ease of use/convenience with potential loss of privacy and security. Issue of social perception.

Standards:
While there remain standardisation efforts (NIST, IEEE, etc) on supporting Cloud federation – there are currently limited standardisation on Cloud security capability. This again limits the potential way in which security capability can be compared across different providers. Although some initial work has been undertaken by US FedRAMP and Cloud Security Alliance along these lines. Similarly, standards such as ISO/IEC WD 27017 Code of practice for information security controls for cloud computing and ISO/IEC CD 27018 Code of practice for data protection controls for public cloud computing services are expected to be completed late 2013, but with the rapid development of cloud technologies and the slow standardization progress, they might be outdated after just a short while.

References

[1] NATO Cybersecurity Reference Manual, 2012. Available at: http://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf. Last access: September 2014.

[2] ENISA – “National Cybersecurity Strategies: Setting the course for national efforts to strengthen security in cyberspace”. Available at: http://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/ENISA%20-%20National%20Cyber%20Security%20Strategies_0.pdf. Last access: September 2014.

[3] Telenor, “Cloud Security White paper”. Available at: http://www.telenor.com/wp-content/uploads/2013/11/TelenorWhitepaperCloud-V_30_v.pdf. Last access: September 2014.

[4] Peter J. Lenk, “NATO’s journey to the Cloud: Vision and Progress”. Available at: https://www.eiseverywhere.com/file_uploads/09fa2f252acff2485fbc52abdfd6171f_NATOCloudforBucharest_CMC_Comms.pdf. Presented at the NATO C4ISR Industry conference, March 2014. Last access: September 2014.

[5] Part of the EPSRC-ESRC funded project “Identifying and Modelling Victim, Business, Regulatory and Malware Behaviours in a Changing Cyberthreat Landscape”. Project partners: Cardiff University (Computer Science, Social Sciences, Mathematics and Business School), Durham University (Social Sciences), City University, London (Computer Science), University of West London (Computer Science), Plymouth University (Computer Science and Psychology).