**Author:** Andrew Cormack**, for the IGF Best Practices Forum on Cybersecurity**

Notes on how cyber-security can affect the achievement of the Sustainable Development Goals (SDGs). Derived from the IGG Policy Options for Connecting and Enabling the Next Billion(s): Phase II. Many of the cyber-security issues affect several SDGs: the connections selected here are chosen as perhaps the best examples of these dependencies.

SDG1 (No Poverty) depends on individuals being able to access information over the Internet. Thus it can be disrupted by weaknesses in, and attacks on, the availability of information services and the networks that individuals use in connecting to them. Issues such as **denial of service attacks** and **services that can act as amplifiers** for them could therefore affect progress towards this goal. Similar issues arise in SDGs 4 (Quality Education), 10 (Reduced Inequalities), 14 (Life below water) & 15 (Life on Land), and the overall aim of providing "meaningful access".

SDG2 (Zero Hunger) includes farmers seeking information, reporting on local conditions, applying for grants etc. Since such activities may involve implicit or explicit criticism of public authorities, they will be hindered by any perception that those authorities are engaged in **surveillance of internet usage**.

SDG3 (Good Health) includes telemedicine, disease monitoring and the storage of patient data. Developed countries have already experienced setbacks in these areas as a result of incidents affecting the **confidentiality and availability of sensitive information** held by medical and health services.

SDG5 (Gender Equality) is harmed by individuals or organisations using communications technologies to engage in **online abuse** and gender-based violence.

SDG6 (Clean Water) involves using communications technologies for the remote monitoring and control of treatment and pumping equipment. **Vulnerabilities in SCADA (Supervisory Control and Data Acquisition) equipment** that is connected to shared networks are a major concern that can turn such automation from a benefit into a serious pollution and health threat.

SDG7 (Affordable and Clean Energy) depends on the widespread acceptance of smart meters and smart grids. Loss of trust in these systems can easily be caused if monitoring equipment and systems do not keep information confidential, or if **information is used for inappropriate purposes**.

SDG8 (Decent Work and Economic Growth) highlights the importance of mobile payment systems, which are critically dependent on the **security of mobile devices** such as phones and tablets.

SDG9 (Industry, Innovation and Infrastructure) suggests that developing countries may find opportunities to develop disruptive industries in the area of IoT (Internet of Things). However **lack of secure development processes** are already causing concerns for IoT and any industry based on them could be severely damaged by a security failure in its products.

SDG11 (Sustainable Cities and Communities). Many of the technical tools suggested as supporting this aim can also become serious threats to individuals and communities if they are not secure. Criminals, neighbours, governments or even family members with **unauthorised access** to internet-monitored home security, traffic monitoring or CCTV systems can cause serious privacy, material, physical or emotional harm.

SDG16 (Peace and Justice) concerns citizen engagement in government, but also notes that these tools can be used for repression and the spread of prejudice. Either will strongly discourage engagement. Systems used to hold authorities to account must be **protected from abuse by those authorities**.