How can Governments be motivated to collaborate internationally to mitigate cybercrime effectively?

There can be little doubt that alongside the significant benefits the Internet delivers to GDP growth, wealth-creation and knowledge-sharing, there exists a pernicious threat to our economic and societal well-being and, potentially, to our safety and security, from a wide range of online criminality.

If we accept for a moment this assessment, what then can governments do, working together, to collectively bring about a reduction in the harm caused by threat actors? What are the key and essential game-changing interventions that governments could implement, if they had the will do to so? And what are the obstacles to be overcome if political leaders decided to work collaboratively in the interests of many nations and not simply pander to their own national interests?

Perhaps our first priority in making the case for strong collaborative inter-governmental working on fighting cybercrime is to identify and target the beneficiaries of this effort – our citizens and SMEs. It might also be helpful to limit the scope of this mission to solving and funding the following key initiatives:

1. To eliminate as far as possible use of the Internet to support online child sexual exploitation. A great deal of work is already underway in this vital area of criminality; it is this on-going effort and the results that have been achieved, that could help pave the way for other cyber crime fighting initiatives. Experience shows that it is a subject that unites politicians, law enforcement officials and citizens in just about every country of the world. It is the cyber glue that could lead to collaborative efforts in other areas which are identified below.
2. To provide online tools, education, training and awareness resources to our citizens and SMEs to help them navigate and transact the Internet in a more safe and secure way. It is not sufficient to expect millions of people to play catch-up and to have the interest or capability to secure their own devices without understanding why, how and with what. We need to generate engaging marketing and communications campaigns that captivate our citizens and that help them understand the risks whilst providing them with the tools, training and knowledge to combat threats and scams that hit their inbox every minute of every day.
3. To strike at the heart of the criminal cyber underground economy by outlawing what are referred to as “alternative payment mechanisms”. Governments have the ability right now, to ban these payment schemes. At the heart of this initiative is a simple premise – at one end of the transaction, a citizen must “buy” the “Internet currency”

whilst at the other end, the criminals must turn the currency into real money by cashing out. If Treasuries and financial institutions around the world were to block those transactions and permit only legitimate UN-recognised currencies to be used on the Internet through regulated payment service provides and cards (such as Visa, MasterCard, AMEX etc), the flow of many US$ Billions to criminal groups would be closed down immediately.

4. To introduce additional legislation, where required, that will enable the confiscation of the proceeds of online crime, including proceeds flowing through any non-UN online currency or financial instrument. These funds could be returned to the victims of crime and used to fund projects which internationally, could bring about a more safe and secure Internet environment for all citizens and SMEs.

Limiting the scope of inter-governmental activity to areas of cyber criminality that are of critical importance to citizens the world over will provide politicians, whose main focus is on re-election, with the raison d’être to act.

By focusing on collaborative activities that will produce tangible and practical solutions for the economic and societal well-being of their nations, we provide leaders with a game-changing platform filled with programmes that will make a real difference to their people and business communities.

By ignoring the sensitive foreign policy issues that see no chance of resolution such as Internet governance and states-sponsored cyber warfare and espionage, we remove from the agenda areas of potential conflict which are very likely to derail any success we might otherwise enjoy.