THE SUBVERSIVE ACTIONS of individuals and groups in our virtual world continue to have destructive implications for our real world. Critical country infrastructure is increasingly targeted; the reputations of organizations and businesses are progressively at risk; and family savings as well as personal identities continue to vanish. New dimensions to this threat have emerged. As cyber-space flourishes alongside mobility, the increased potential of smartphones and tablets means these individuals and groups can seamlessly target their victims while crossing physical space and sovereign borders.

Progress towards countering this dark reality is promising, but slow. Best practices and shared objectives regarding cybersecurity have been cautiously distributed and absorbed worldwide. While some countries are recognizing the gravity of these threats and forming advantageous cross-sectoral partnerships to suppress them, others are unwilling or unable to do so. At the same time, the general public is growing more aware of the risks it faces, but is overwhelmed by the amount and complexity of information available.

The stakes are too high for progress to stall. More countries must share this heightened sense of urgency if the international community wishes to act effectively. One cannot honestly expect to combat threats that cut across borders, cultures, languages, and histories with a weak global response. One of the most practical measures we can take is to not only improve the ability of all countries to hold these malicious individuals and groups accountable, but also help their citizens protect themselves. In fighting this global threat, we are, after all, only as strong as our weakest link.

A level playing field where we share the same basic tools and knowledge is within reach, which is why the international law enforcement community is committed to training experts who can investigate these threats and collect evidence that can lead to prosecutions. We are simultaneously boosting the capabilities of these experts and resources available to them through collaboration with public organizations and private sector companies. Collaboration thus far has yielded better integration with CERTs, as well as mutually beneficial partnerships like those between INTERPOL, anti-malware vendor Kaspersky Lab, and IT-communications firm NEC Corporation.

Our efforts will continue alongside and joined to the efforts in other sectors, with the shared vision of a safe, stable, and predictable cyberspace in mind. However, only by working together will our individual comparative advantages emerge as a collective advantage decisive enough to positively alter the reality in which we currently live. Our future economic and social wellbeing depends on it, and our colleagues and clients, as well as their families and children, certainly deserve it.

Ron Noble
INTERPOL Secretary General