The Information and Communication Technology (**ICT**) sector is one of many sectors that cannot avoid the disruptions caused by the Covid-19 pandemic. Cyberattacks in the sector have risen significantly, raising the need for countries and industries to improve ICT supply chain resilience.

Resilience is all about resistance and recovery. Stakeholders must build management systems based on avoidance and containment capabilities. Meanwhile, stakeholders must also pay attention to stabilization and return for recovery. For example, we could see that the chip processor industry is currently experiencing “doomsday” problems caused by Covid-19-induced lack of supply despite recovery in global demand. Thus, resistance to shocks and recovery is crucial to ensure resilience.

The ICT sector should not only provide solutions to other industries, but must itself ensure risk management that can improve ICT supply chain resilience, especially to face the threat of disruption during and after the COVID-19 pandemic.

The United States’ Cybersecurity and Infrastructure Security Agency (CISA) found that the vulnerability in the ICT sector was caused by unreliable state actors (46%), lack of short-term and long-term planning (40%) and geographic factors (36%). The data showed similarities to Indonesia, particularly on unreliable state actors. In addition, CISA also found several major risks to the ICT sector, namely: the Covid-19 pandemic (76%), cyberattacks (44%), government sanctions (36%) and natural disasters (30%). As we know, the cyber infrastructure of the Indonesian government has been the main target of hackers during the pandemic, which has significant impact on the ICT Sector.

One way for both government and non-government stakeholders to minimize these risks is to improve cybersecurity capabilities, which will subsequently improve ICT supply chain resilience. However, this will be constrained if all relevant parties do not improve the cybersecurity of their systems. The main obstacle is the lack of understanding surrounding the importance of cybersecurity to increase ICT supply chain resilience. In the end, stakeholders must consider significant investment to increase the overall standard of cybersecurity to improve the resilience of the ICT supply chain.

Dr. Pratama Persadha was born in Blora, October 14, 1977. His career began when he entered the State Code Academy (Aksara) in 1996 and graduated in 1999. At that time, Pratama immediately started his career at the National Code Institute (Lemsaneg).

At a relatively young age, in his early 30s, Pratama has become the Director of Pamsignal of the National Crypto Agency, as well as the Head of the Lemsaneg IT Team for the General Elections Commission (KPU) and also the Presidential IT Team.

In 2014, Pratama chose to retire from Lemsaneg and established a cybersecurity research institute CISSReC (Communication & Information System Security Research Center). At CISSReC, he became widely known among the public through his statements in various Indonesian media.

Pratama is now widely recognized as one of the cybersecurity experts in Indonesia. Pratama has advocated for the establishment of National Cyber and Crypto Agency (BSSN) since 2015, long before the establishment of the Agency. He is also advocating for the passage of Personal Data Protection Bill currently deliberated in the Indonesian parliament.

In addition, Pratama is also active as a lecturer in several institutions including State Intelligence Academy (STIN), National Resilience Institute (Lemhanas), Police Staff College (PTIK), among others.