Rilis Media

KOLABORASI
MULTI PEMANGKU KEPENTINGAN
UNTUK KEAMANAN SIBER DALAM PEMILU 2019

Network for Democracy and Electoral Integrity
(NETGRIT)

NETGRIT dan *International Insitute for Democracy and and Electoral Assistance* (IDEA) menggelar diskusi publik dengan tema "Tantangan Keamanan Siber dalam Pemilu 2019"., Kamis, 6 Desember 2018. Hadir sebagai pembicara: Viryan (Komisioner KPU RI), Peter Wolf (IDEA), Nuriman (Perwakilan Paslon Prabowo-Sandi), Setiadi yazid (Centre for Cyber Security and Cryptography, Univ. Indonesia), dan Riko Rasota Rahmada (Kemkominfo).

Keamanan siber dalam penyelenggaraan pemilu 2019 sangat penting diperhatikan. Pengalaman penyelenggaraan pemilu di dunia dan praktik di Indonesia, ancaman keamanan siber sesuatu yang nyata. Belanda, Amerika dan Perancis menjadi contoh beberapa negara yang pernah berhadapan dengan ancaman keamanan siber dalam penyelenggaraan pemilu. Di Indonesia setelah pemilu 2014, Pilkada 2015 dan 2017, untuk pertama kalinya hasil pilkada 2018 tidak berhasil ditampilkan dalam sistem informasi penghitungan suara (SITUNG) karena serangan siber.

Studi komparasi, spektrum ancaman siber terkait kepemiluan mengambil beberapa bentuk: (1) tingkat rendah, kemungkinan serangan peretasan secara acak, (2) upaya peretasan terarah (advanced perceived threats), (3) eksploitasi tantangan khusus kepemiluan, dan (4) disinformasi dan operasi penyebaran pengaruh.

Peretasan dan disinformasi menjadi ancaman utama keamanan siber atas proses kepemiluan. Ancaman tersebut dapat menyerang terhadap semua pemangku kepentingan: penyelenggara pemilu, peserta pemilu, dan publik. Peretasan menyerang infrastruktur kepemiluan melalui beberapa cara diantaranya *hacking, social engineering, internal attack and breaches, virus/malware/botnet, dan ransomeware and exertortion*. Sementara itu disinformasi melakukan penggiringan opini yang sifatnya merusak. Keseluruhan ancaman tersebut - peretasan dan disinformasi - berujung pada delegitimasi terhadap proses pemilu.

Pengalaman banyak negara, penyelenggara pemilu hanya bertanggungjawab atas 25% dari resiko siber. Selebihnya adalah ditanggung oleh institusi atau pemangku kepentingan lainnya. Oleh karena itu, penggabungan sumberdaya, keahlian dan intelijen siber yang dilakukan secara terbuka menjadi kunci keamanan siber dalam pemilu.

KPU merupakan lembaga yang bersifat mandiri. Namun demikian, KPU tidak bisa bekerja sendiri menghadapi ancaman keamanan siber karena keterbatasan kemampuan yang dimiliki: infrastruktur, sumberdaya, dan keahlian. Oleh karena itu, penyelenggara pemilu harus membangun kolaborasi dengan peserta pemilu, pemerintah, dan masyarakat sipil, bahkan jika diperlukan dunia internasional untuk memastikan keamanan siber dalam penyelenggaraan pemilu. Kolaborasi tersebut dilakukan secara terbuka dan terukur dengan menempatkan KPU sebagai aktor utama yang mengkoordinasikan.

Persoalan ancaman siber dalam pemilu bukan persoalan hasil pemilu, sebab hasil pemilu di Indonesia berbasis rekapitulasi manual. Yang lebih substantif ancaman itu dapat mengganggu kepercayaan publik, sistem demokrasi dan kehidupan berbangsa.

Sigit Pamungkas
Direktur Eksekutif