UNIVERSITAS
GADJAH MADA
**Analisis Sosio - Teknis Tata Kelola Keamanan Siber Sektor Publik Indonesia (Studi Kasus pada Badan
Kepegawaian Negara)**
ANINDA ISNAINI, Dr. Bevaola Kusumasari, M.Si.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

ABSTRAK

Penelitian ini bertujuan untuk menganalisis kondisi tata kelola keamanan siber di Badan Kepegawaian Negara (BKN) serta menjelaskan hubungan keterkaitan antara faktor teknis dan faktor sosial dalam membentuk tata kelola keamanan siber melalui perspektif *Socio-Technical System* (STS). Kajian tata kelola keamanan siber dalam ranah administrasi publik masih relatif terbatas, dan penelitian terdahulu cenderung mengidentifikasi faktor-faktor secara parsial tanpa banyak menjelaskan interaksi antara aspek teknis dan sosial, khususnya pada organisasi sektor publik di negara berkembang. Penelitian ini menggunakan metode kualitatif dengan pendekatan studi kasus pada BKN, dengan pengumpulan data melalui wawancara mendalam, analisis dokumen, dan observasi lapangan terhadap informan di Kantor Pusat dan beberapa Kantor Regional BKN. Hasil penelitian menunjukkan bahwa BKN telah memiliki kebijakan, struktur pengelolaan, dukungan sumber daya, dan program budaya keamanan siber sebagai fondasi tata kelola, namun implementasinya masih menghadapi tantangan seperti keterbatasan sumber daya manusia berkompetensi khusus, belum optimalnya integrasi teknologi keamanan, kesenjangan antara kebutuhan teknis dan keputusan investasi, serta internalisasi budaya keamanan yang belum merata di seluruh unit. Melalui perspektif STS, penelitian ini mengidentifikasi empat pola interaksi antara sistem teknis dan sistem sosial, yaitu: (1) pertumbuhan kapasitas teknis mendorong tuntutan terhadap sistem sosial; (2) sistem sosial menentukan tingkat optimalisasi dan efektivitas sistem teknis; (3) persepsi berperan sebagai mekanisme penghubung interaksi kedua sistem; dan (4) kesenjangan sosio-teknis maupun keselarasan (*joint optimization*) yang timbul dari interaksi tersebut. Temuan ini menegaskan bahwa efektivitas tata kelola keamanan siber ditentukan oleh keselarasan interaksi antara sistem teknis dan sistem sosial secara berkelanjutan, bukan oleh keunggulan salah satu sistem semata. Penelitian ini memberikan kontribusi teoretis bagi pengembangan kajian tata kelola keamanan siber sektor publik melalui pendekatan STS, serta kontribusi praktis bagi BKN dalam memperkuat kebijakan, sumber daya, dan budaya keamanan siber secara terpadu.

Kata kunci: *tata kelola keamanan siber, Socio-Technical System, sektor publik, Badan Kepegawaian Negara, studi kasus*

UNIVERSITAS
GADJAH MADA
**Analisis Sosio - Teknis Tata Kelola Keamanan Siber Sektor Publik Indonesia (Studi Kasus pada Badan
Kepegawaian Negara)**
ANINDA ISNAINI, Dr. Bevaola Kusumasari, M.Si.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

ABSTRACT

*This study aims to analyze the condition of cybersecurity governance at the National Civil Service Agency (*Badan Kepegawaian Negara*/BKN) and to describe the relationship between technical and social elements in the formation of cybersecurity governance through the Socio-Technical System (STS) perspective. Research on cybersecurity governance in the field of public administration is still relatively limited, and previous studies tend to identify influencing factors partially without adequately explaining the interaction between technical and social aspects, especially within public sector organizations in developing countries. This study used a qualitative method with a case study approach at BKN. Data were gathered through in-depth interviews, document analysis, and field observation involving informants from BKN's Head Office and several Regional Offices. The findings show that BKN has established its governance through policies, organizational structures, resource support, and cybersecurity culture programs. But implementation still faces challenges, including limited human resources with specialized cybersecurity competencies, suboptimal integration of security technologies, gaps between technical needs and investment decisions, and uneven internalization of security culture across units. Through the STS perspective, this study identifies four interaction patterns between the technical and social systems: (1) the growth of technical capacity increases demands on the social system; (2) the social system determines the extent to which technical capacity is optimized and rendered effective; (3) perception functions as the mechanism linking the interaction between the two systems; and (4) socio-technical gaps and alignment (joint optimization) emerge as consequences of these interactions. These findings affirm that the effectiveness of cybersecurity governance is determined by the sustained alignment between technical and social systems, rather than by the superiority of either system alone. This study contributes theoretically to the development of public sector cybersecurity governance studies through the STS approach, and practically by providing BKN with a basis for strengthening its policies, resources, and security culture in an integrated manner.*

Keywords: *cybersecurity governance, Socio-Technical System, public sector, National Civil Service Agency, case study*