1. Record Nr. UNINA9910299352703321

Autore	Schallbruch Martin
Titolo	Cybersecurity in Germany / / by Martin Schallbruch, Isabel Skierka
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2018
ISBN	3-319-90014-5
Edizione	[1st ed. 2018.]
Descrizione fisica	1 online resource (VIII, 66 p.)
Collana	SpringerBriefs in Cybersecurity, , 2193-973X
Classificazione	32.24.56 08.12.16
Disciplina	005.8
Soggetti	Computer security Computers and civilization Public policy Systems and Data Security Computers and Society Public Policy
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	Intro; foreword; contents; 1 Introduction; 1.1 On Terminology; 1.2 Approach; 1.3 Peculiarities of the German political system; 1.4 Structure; references; 2 The German view on cybersecurity; 2.1 The public perception of cyber issues; 2.2 Political and regulatory concepts; 2.3 Snowden and the emerging discussion about technological sovereignty; 2.4 Combining a German data protection and engineering approach with holistic cyber debates; 2.5 Advantages and disadvantages of the German approach-A preliminary balance; references; 3 The evolution of German cybersecurity strategy; 3.1 Introduction 3.2 Phase 1, 1991-2011: IT security and critical infrastructure protection 3.3 Phase 2: 2011-2016: building a civilian cybersecurity strategy; 3.3.1 The first national cybersecurity strategy for Germany; 3.3.2 The IT security law; 3.3.3 The Snowden revelations; 3.4 Phase 3, 2016-2018: consolidating a comprehensive civilian-military approach to cybersecurity; 3.4.1 The 2016 white paper on German security policy and the future of the Bundeswehr; 3.4.2 The 2016 second national

cybersecurity strategy; 3.4.3 Taking stock of past developments for future cybersecurity strategies; references
4 The organisation of cybersecurity in Germany 4.1 Particularities of German law enforcement, intelligence, and public security organisations; 4.2 The German military's role in the cyber realm; 4.3 Cooperation and conflict between agencies; 4.4 Public-private cybersecurity cooperation; references;
5 Current priorities and gaps in German national cybersecurity, future trends; 5.1 Introduction; 5.2 Legal, technical and practical development of active cyber defence; 5.3 Cybersecurity architecture-roles and responsibilities of agencies; 5.4 Towards a governmental vulnerability handling strategy 5.5 Implementing a comprehensive IT security industry policy 5.6 Finding a coherent legal concept for safety and security; 5.7 International cooperation; references;
6 Conclusion

Sommario/riassunto

In 2016, Germany's government presented its third cybersecurity strategy, which aims to strengthen the national cyber defence architecture, cooperation between the state and industry, and individual users' agency. For many years, Germany has followed/adopted a preventive and engineering approach to cybersecurity, which emphasizes technological control of security threats in cyberspace over political, diplomatic and military approaches. Accordingly, the technically oriented Federal Office for Information Security (BSI) has played a leading role in Germany's national cybersecurity architecture. Only in 2016 did the military expand and reorganize its cyber defence capabilities. Moreover, cybersecurity is inextricably linked to data protection, which is particularly emphasised in Germany and has gained high public attention since Edward Snowden's revelations. On the basis of official documents and their insights from many years of experience in cybersecurity policy, the two authors describe cyber security in Germany in the light of these German peculiarities. They explain the public perception of cybersecurity, its strong link with data protection in Germany, the evolution of Germany's cybersecurity strategies, and the current organisation of cybersecurity across the government and industry. The Brief takes stock of past developments and works out the present and future gaps and priorities in Germany's cybersecurity policy and strategy, which will be decisive for Germany's political role in Europe and beyond. This includes the cybersecurity priorities formulated by the current German government which took office in the spring of 2018.