
Cyber resilience: A review of critical national infrastructure and cyber security protection measures applied in the UK and USA.

Authors: Harrop, Wayne¹ *w.harrop@coventry.ac.uk*
Matteson, Ashley¹ *ashmatteson@hotmail.com*

Source: Journal of Business Continuity & Emergency Planning. Winter2013/2014, Vol. 7 Issue 2, p149-162. 14p. 3 Charts.

Document Type: Article

Subject Terms: *COMPUTER network security
*CYBERTERRORISM
*COMPUTER security
PREVENTION

Geographic Terms: UNITED States
GREAT Britain

Author-Supplied Keywords: 1o7 US Cyber Security Act 2012
C/KR
CNI
cyber security
cyberattacks
DDoS
national security

Abstract: This paper presents cyber resilience as key strand of national security. It establishes the importance of critical national infrastructure protection and the growing vicarious nature of remote, well-planned, and well executed cyber attacks on critical infrastructures. Examples of well-known historical cyber attacks are presented, and the emergence of 'internet of things' as a cyber vulnerability issue yet to be tackled is explored. The paper identifies key steps being undertaken by those responsible for detecting, deterring, and disrupting cyber attacks on critical national infrastructure in the United Kingdom and the USA. [ABSTRACT FROM AUTHOR]

Copyright of Journal of Business Continuity & Emergency Planning is the

property of Henry Stewart Publications LLP and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use. This abstract may be abridged. No warranty is given about the accuracy of the copy. Users should refer to the original published version of the material for the full abstract. (Copyright applies to all Abstracts.)

Author ¹Centre for Disaster Management, Coventry University, Priory Street,
Affiliations: Coventry CV1 5FB. UK

ISSN: 1749-9216

Accession 94779804

Number: