FIBAA

Description of Course Unit according to the ECTS User's Guide 2015

Course unit title	**Genius Weapons and Cyber Security**
Course unit code	HI191411
Type of course unit (compulsory, optional)	Optional
Level of course unit (according to EQF: first cycle Bachelor, second cycle Master)	First cycle Bachelor
Year of study (if applicable)	3rd Year
Semester/trimester when the course unit is delivered	6th semester
Number of ECTS credits allocated	4.83 ects
Name of lecturer(s)	1. Renitha Dwi Hapsari, M.Hub.Int. email: renithadwi.hi@upnjatim.ac.id Office hours: mon-fri, 09.00-16.00 2. Prihandono Wibowo, M.Hub.Int. email: prihandono_wibowo.hi@upnjatim.ac.id Office hours: mon-fri, 09.00-16.00
Learning outcomes of the course unit	1. Students demonstrate sufficient knowledge and understanding on international relations and future of warfare 2. Students demonstrate sufficient knowledge and understanding on smart & genius weapon, cyber security, the position of Big Power and Developing Countries on this issues 3. Students demonstrate sufficient knowledge and understanding the importance of new mechanism and strategies to control and prevent future catastrophes
Mode of delivery (face-to-face, distance learning)	Face to face / Online learning (ilmu.upnjatim.ac.id)

Prerequisites	N/A
Course contents	For 14 weeks, students will learn: 1. International Relations and Future Threats and Warfare 2. Air and Space Power and Control 3. Smart and Genius Weapons: Good and Bad Used 4. Web Activism and the Internet as Weapon 5. Russia and China Power 6. US Power 7. Non-state Actors: Cyber-terrorism, Black Market, Civil Disobedience 8. Scenario in Southeast Asia 9. Scenario in Middle East 10. Scenario in Africa 11. Threat Detection, Prevention and Mitigation 12. Genius Weapons and Cyber Attacks on IHL Perspectives 13. Indonesian Context: Opportunities and Challenges
Recommended or required reading	Required reading: 1. Del Monte, Louis A. 2018. *Genius Weapons: Artificial Intelligence, Autonomous Weaponry, and the Future of Warfare*. New York: Prometheus Books. 2. Wills, Collin. 2015. *Unmanned Combat Air Systems in Future Warfare Gaining Control of the Air*. London: Palgrave MacMillan 3. O' Hanlon, Michael E.. 2015. *The Future of Land Warfare*. Washington DC: Brookings Institution Press 4. Knapp, Kenneth J.. 2009. *Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions (Advances in Information Security and Privacy)*. New York: Information Science Reference 5. Karatzogianni, Athina. 2008. *Cyber-Conflict and Global Politics*. New York: Routledge 6. Mitra, Ananda. 2010. *Digital Security: Cyber Terror and Cyber Security (The Digital World)*. New York: Infobase Publishing 7. Gori, U. 2009. *Modelling Cyber Security: Approaches, Methodology, Strategies - Volume 59 NATO Science for Peace and Security Series - E: Human and Societal Dynamics*. Amsterdam: IOS Press 8. Clarke, Richard A. and Robert Knake. 2010. *Cyber War: The Next Threat to National Security and What to Do About It*. HarperCollins 9. Andress, Jason and Steve Winterfeld. 2011. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Syngress
Planned learning activities and teaching methods	Lecture and blended-learning consists of discussions, case studies and project-based examination.

	Mid-term exam : 2000 words study case essay Final exam: 3000 words Policy Brief
Language of instruction	Indonesia-English
Work placement(s)	N/A