In 1986, astronomer Clifford Stoll discovered a 75-cent billing disparity in the accounting software of Lawrence Berkeley Laboratory, which led to the discovery of hackers accessing US military computers and data.The computer security community was initially divided between academic conferences and practical applications, leading to a lack of understanding of the field and insufficient time for implementing security measures.Despite notifying government agencies, the government failed to act, and it took Stoll over a year to track the hackers to Germany, where they were selling US military information to the Soviet Union.Private individuals like Stoll took personal responsibility for technologies and projects, assuming the role of cybersecurity experts.The 1984 Counterfeit Access Device and Computer Fraud and Abuse Act, which outlawed hacking, was more successful, but limited to domestic attacks and did not make computers more secure.This incident highlights the state of cybersecurity in 1986, where government agencies were responsible but failed to see the threat posed by networks between computers.The paper examines the influence of the cybersecurity community on government funding, projects, standards, and laws, and how the government influenced the community.